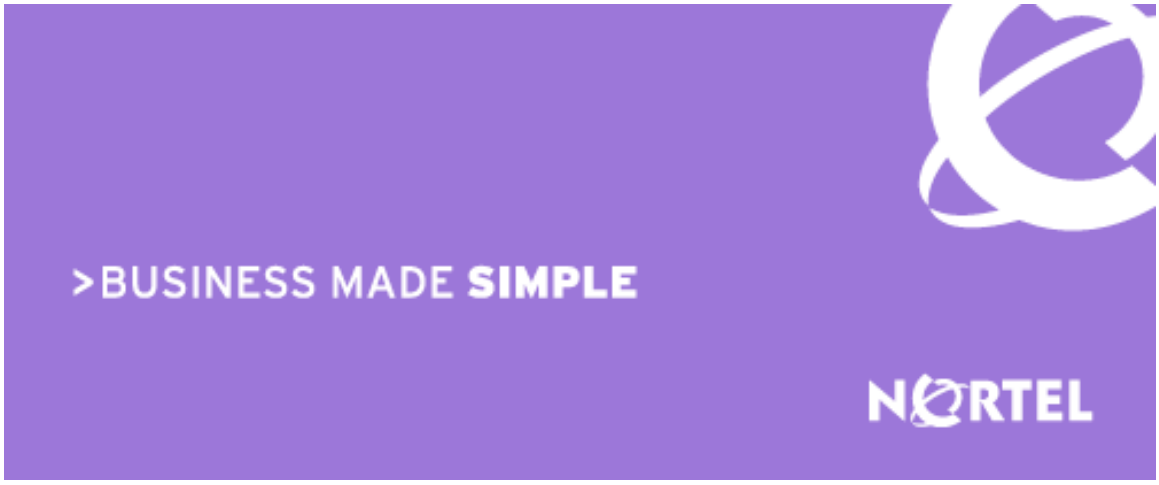


Identity Engines Ignition Server
Ethernet Routing Switch
8600 8300 1600 5500 5600 4500 2500
Engineering

> Switch User Authentication using Identity Engines Ignition Server Technical Configuration Guide

Enterprise Networking Solutions
Document Date: October 2009
Document Number: NN48500-589
Document Version: 1.0

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at www.nortel.com.

Copyright © 2009 Nortel Networks. All Rights Reserved.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice. Nortel Networks, the Nortel Networks logo and the Globemark are trademarks of Nortel Networks.

Abstract

Revision Control

No	Date	Version	Revised by	Remarks
1	10/09/2009	1.0	JVE	Initial release

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.

External Distribution

TABLE OF CONTENTS

CONVENTIONS **4**

1. OVERVIEW: RADIUS USER AUTHENTICATION USING IDENTIFY ENGINES **5**

1.1 RADIUS SUPPORT ON NORTEL SWITCHES 5
1.2 USER AUTHENTICATION USING ERS1600, ERS8300, OR ERS8600 5
1.3 USER AUTHENTICATION USING ERS5600, ERS5500, ERS4500, OR ERS2500 6

2. ERS8600 SWITCH CONFIGURATION EXAMPLE **7**

2.1 PART 1: BASIC AAA CONFIGUATION 8
2.1.1 ERS8600 Configuration *8*
2.1.1.1 Add out-of-band IP address 8
2.1.1.2 Enable RADIUS 8
2.1.2 ERS 8600 Switch: Verify Operations *9*
2.1.2.1 Verify RADIUS Global Settings 9
2.1.3 IDE Setup *10*
2.1.3.1 Configure an Outbound Attribute on Ignition Server for VLAN 10
2.1.3.2 Add Users 18
2.1.3.3 Add an Access Policy 22
2.1.3.4 Add the Nortel ERS8600-1 switch as an RADIUS Authenticator 41
2.1.4 Verification *44*
2.1.4.1 Verify User Authentication 44
2.1.4.2 Verify user authentication from ERS switch 45
2.2 PART 2: ERS8600 CONFIGURATION WITH SPECIFIC COMMANDS DISABLED 48
2.2.1 ERS8600 Configuration *48*
2.2.2 IDE Setup *49*
2.2.2.1 Configure Outbound attributes to deny ERS8600 CLI commands 49
2.2.2.2 Modify the Authorization Policy for the ERS8600 read-write user 57
2.2.3 Verification *60*

3. ERS5600 SWITCH CONFIGURATION EXAMPLE **61**

3.1 ERS5600 CONFIGURATION 62
3.1.1 Enable RADIUS *62*
3.2 IDE SETUP 63
3.2.1 Configure an Outbound Attribute on Ignition Server for Service-Type *63*
3.2.2 Add Users *69*
3.2.3 Add Access Policy *72*
3.2.4 Add the Nortel ERS5600-1 switch as an RADIUS Authenticator *87*
3.3 VERIFICATION 90
3.3.1 Verify User Authentication *90*
3.3.2 Verify user authentication from ERS switch *91*

4. SOFTWARE BASELINE **94**

5. REFERENCE DOCUMENTATION **94**

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.

External Distribution

Conventions

This section describes the text, image, and command conventions used in this document.

Symbols:

Tip – Highlights a configuration or technical tip.

Note – Highlights important information to the reader.

Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

Text:

Bold text indicates emphasis.

Italic text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

ERS5520-48T# ***show running-config***

Output examples from Nortel devices are displayed in a Lucinda Console font:

ERS5520-48T# ***show running-config***

```
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 5520-24T-PWR
! Software version = v5.0.0.011
enable
configure terminal
```

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

1. Overview: RADIUS User Authentication using Identify Engines

This document provides the framework for implementing user Authentication, Authorization, and Accounting for Nortel switches.

1.1 RADIUS Support on Nortel Switches

	RADIUS authenti-cation	802.1x (EAP) RADIUS authenti-cation	RADIUS accoun-ting	802.1x (EAP) RADIUS account-ing	RADIUS account-ing for CLI commands	RADIUS user access profile	RADIUS SNMP account-ing
ERS 8600	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ERS 8300	Yes	Yes	Yes	Yes	Yes	Yes	No
ERS 1600	Yes	Yes	Yes	Yes	Yes	Yes	No
ES 460/470	Yes	Yes	No	No	No	No	No
ERS 2500	Yes	Yes	No	Yes	No	No	No
ERS 4500	Yes	Yes	No	Yes	No	No	No
ERS 5500	Yes	Yes	No	Yes	No	No	No
ERS 5600	Yes	Yes	No	Yes	No	No	No

1.2 User Authentication using ERS1600, ERS8300, or ERS8600

The ERS1600, ERS8300, and ERS8600 each support six different user access levels. The access level is determined by the RADIUS attribute value sent back to the switch. The switch uses RADIUS Vendor-Specific Attributes (IETF Attribute 26) to support its own extended attributes. Vendor identifier 1584 (Bay Networks) attribute type 192 is used where the value is a number from 0 to 6. The following chart displays the RADIUS attribute values and corresponding access level.

Access Level	VSA Attribute 26 – Vendor Identifier 1584 Type 192 value
None-Access	0
Read-Only-Access	1
Layer 1-Read-Write-Access	2
Layer 2-Read-Write-Access	3
Layer 3-Read-Write-Access	4
Read-Write-Access	5
Read-Write-All-Access	6

In addition, on the ERS8600 only, via vendor identifier 1584 attribute type 194, if is set to a value of 0, you can enter a list of CLI commands not allowed for a user. The CLI command is entered using the RADIUS string value configured via RADIUS vendor identifier 1584 attribute type 195.

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

1.3 User Authentication using ERS5600, ERS5500, ERS4500, or ERS2500

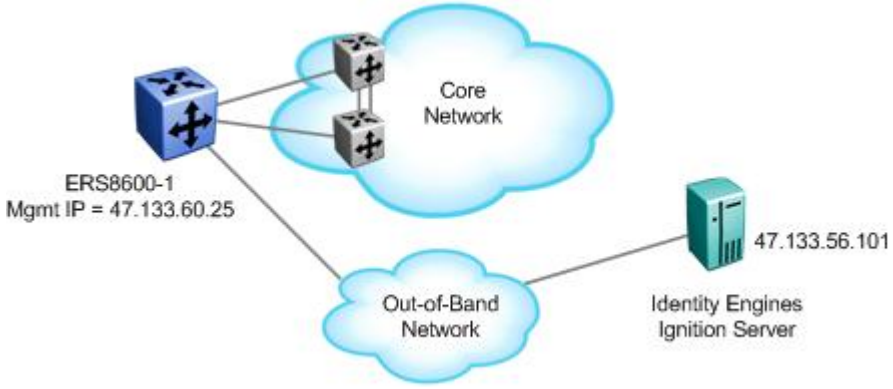
The ERS5600, ERS5500, ERS4500, and ERS2500 each support two different user access levels which are read-only or read-write. RADIUS attribute type 6, Service-Type, is used to determine the access level. The following displays the complete list of RADIUS attribute values for the RADIUS Service-Type attribute where value 6 (Administrative) is used for read-write access and value 7 (NAS Prompt) is used for read-only access

```
Sub-registry: Values for RADIUS Attribute 6, Service-Type
Reference: [RFC2865][RFC3575]
Registration Procedures: IETF Consensus

Registry:
Value  Description                      Reference
-----  -------------------------------  ---------
1      Login
2      Framed
3      Callback Login
4      Callback Framed
5      Outbound
6      Administrative
7      NAS Prompt
8      Authenticate Only
9      Callback NAS Prompt
10     Call Check
11     Callback Administrative
12     Voice                            [Chiba]
13     Fax                              [Chiba]
14     Modem Relay                      [Chiba]
15     IAPP-Register                    [IEEE 802.11f][Kerry]
16     IAPP-AP-Check                    [IEEE 802.11f][Kerry]
17     Authorize Only                   [RFC3576]
18     Framed-Management                [RFC5607]
```

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.

External Distribution

2. ERS8600 Switch Configuration Example



For this configuration example, we will enable RADIUS user authentication on ERS8600-1 using the out-of-band management port. We will configure the Identity Engines RADIUS server with the following three users:

- User name with read-only access: 8600ro
- User name with read-write access: 8600rw
- User name with read-write-all access: 8600rwa

For this example, we will break down the configuration into two parts. In part one, we will simply add AAA services for the three users shown above. Part two is a continuation of part one with the addition of showing how to restrict certain CLI commands. In part two, we will pick the read-write user and deny access to QoS and filter configuration for this user.

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

2.1 Part 1: Basic AAA Configuation

2.1.1 ERS8600 Configuration

Assuming we are using the out-of-band management port.

2.1.1.1 Add out-of-band IP address

ERS8600-1 Step 1 – Add out-of-band IP address and route

```
ERS-8606:5# config bootconfig net mgmt ip 47.133.60.25/24
ERS-8606:5# config bootconfig net mgmt route add 47.0.0.0/8 47.133.60.1
```

2.1.1.2 Enable RADIUS

ERS8600-1 Step 1 – Add RADIUS server, enable RADIUS, and enable RADIUS accounting

```
ERS-8606:5# config radius server create 47.133.56.101 secret nortel priority 1
ERS-8606:5# config radius enable true
ERS-8606:5# config radius acct-enable true
ERS-8606:5# config radius acct-include-cli-commands true
```

When configuring the RADIUS server on the ERS8600, you can configure the switch with a RADIUS source-IP address which in turn will be the IP address used for RADIUS requests. The RADIUS source-IP address must be a circuit-less IP address (CLIP) or otherwise known as a loopback address. If you do not enable a RADIUS source-IP address, by default, the ERS8600 uses the IP address of the outgoing interface as the source IP address for RADIUS. Unfortunately, although you can create and enable a RADIUS source-IP when using the out-of-band management port, this feature is not supported on the out-of-band management port. Hence, if you have two CP cards, you will have to configure two RADIUS Authenticators on the RADIUS server.

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

2.1.2 ERS 8600 Switch: Verify Operations

2.1.2.1 Verify RADIUS Global Settings

Step 1 – Verify that RADIUS has been enabled globally

```
ERS-8606:5# show radius info
```

Result:

```
       Sub-Context: clear config dump monitor mplsping mplstrace peer show
       switchover test trace
       Current Context:

                    acct-attribute-value : 193
                            acct-enable : true
                acct-include-cli-commands : true
                access-priority-attribute : 192
                     auth-info-attr-value : 91
                 command-access-attribute : 194
                   cli-commands-attribute : 195
                            cli-cmd-count : 40
                       cli-profile-enable : false
                                   enable : true
                         igap-passwd-attr : standard
                   igap-timeout-log-fsize : 512
                                maxserver : 10
                    mcast-addr-attr-value : 90
                            sourceip-flag : false
```

Via 8600-1, verify the following information:

Option	Verify
Acct-enable acct-include-cli-commands	Verify that the CLI accounting is set to ***true*** globally
enable	Verify that enable is set to ***true*** globally telling us that RADIUS is enabled

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

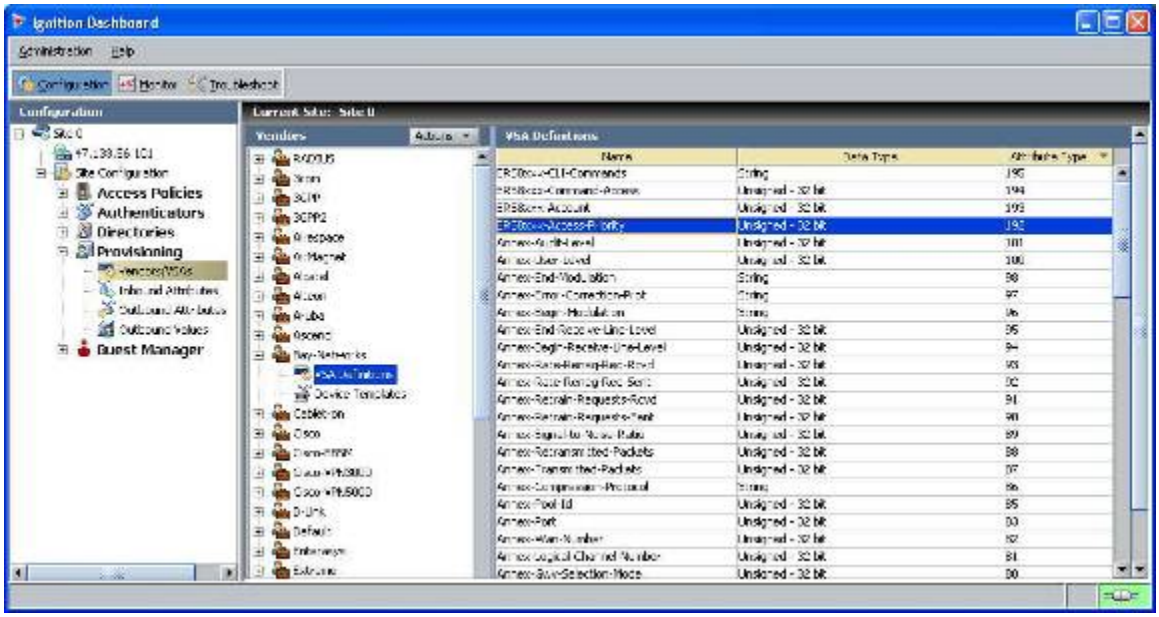
2.1.3 IDE Setup

2.1.3.1 Configure an Outbound Attribute on Ignition Server for VLAN

The following chart displays the outbound attribute values required by the ERS8600 for each access level for RADIUS vendor identifier 1584 (Bay Networks) attribute type 192. For this example, we will configure IDE with attribute values of 1, 5, and 6.

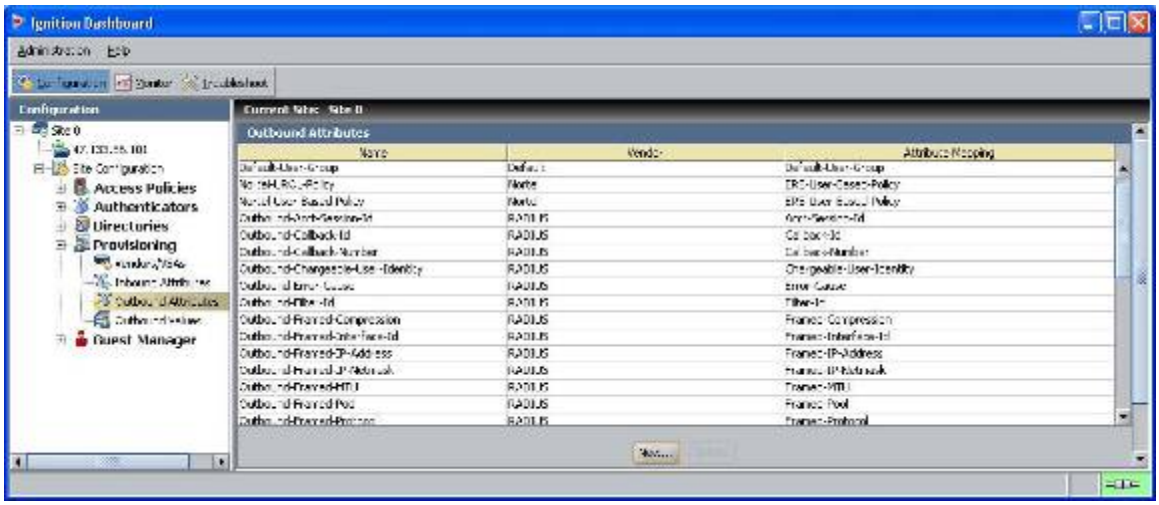
Access Level	Attribute Value	User Name
None-Access	0	
Read-Only-Access	**1**	**8600ro**
L1-Read-Write-Access	2	
L2-Read-Write-Access	3	
L3-Read-Write-Access	4	
Read-Write-Access	**5**	**8600rw**
Read-Write-All-Access	**6**	**8600rwa**

IDE Step 1 – IDE already has the vendor specific attributes defined (Bay Networks vendor code 1584 using attribute type 192) for the ERS8600 which can be viewed by going to *Site Configuration -> Provisioning -> Vendors/VSAs -> Bay-Networks -> VSA Definitions.*



 Copyright © 2009 Nortel Networks. All Rights Reserved.

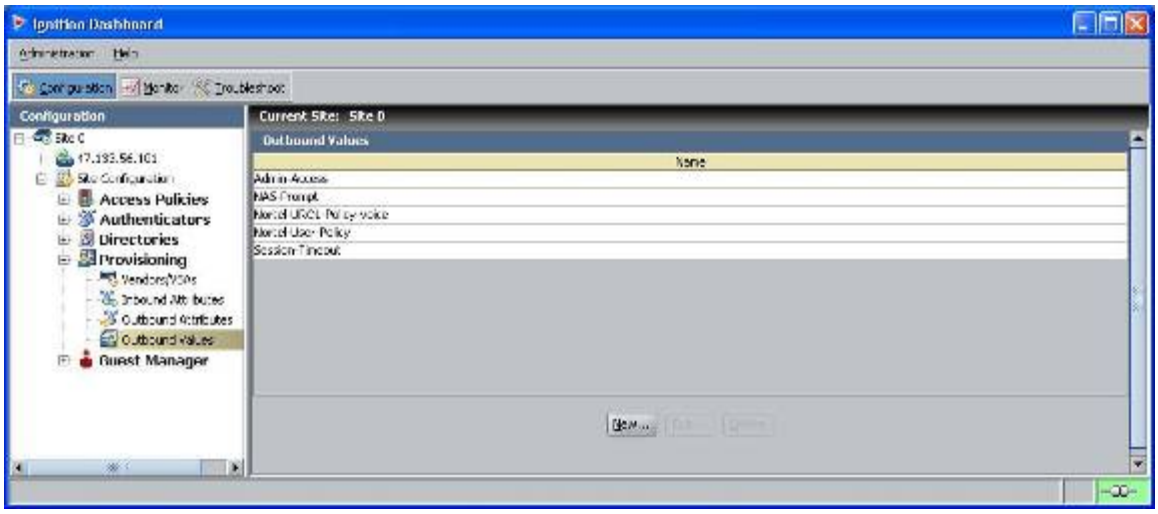
IDE Step 2 – Go to *Site Configuration -> Provisioning -> Outbound Attributes -> New*



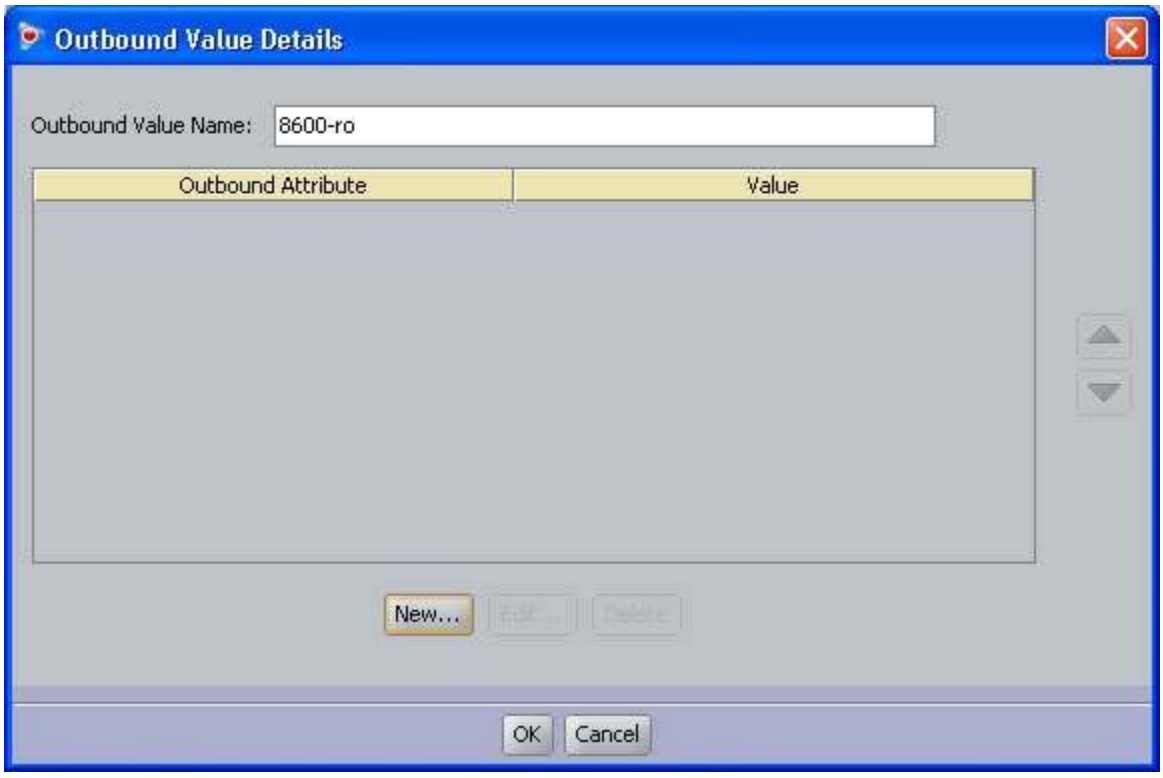
IDE Step 3 – Via the *Outbound Attribute* window, type in a name for the attribute to be used for access priority (i.e. ERS8600-Access-Priority as used in this example), click the *VSA* radio button, select *Bay-Networks* via *Vendor* and *ERS8xxx-Access-Priority* via *VSA*. Click on *OK* when done

 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 4 – Go to *Site Configuration -> Provisioning -> Outbound Values -> New*

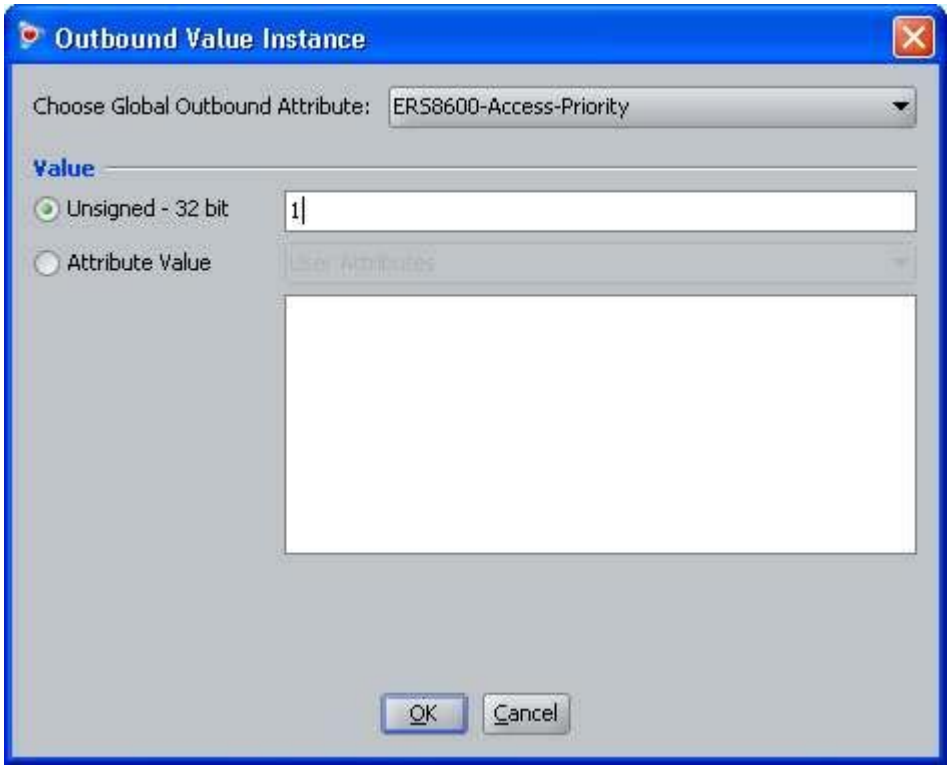


IDE Step 5 – Using the Outbound Attribute created in Step 3, we will first add an attribute value of 1 for read-only-access. Start by entering a name via the *Outbound Value Name:* window (i.e. *8600-ro* as used in this example) and click on *New*



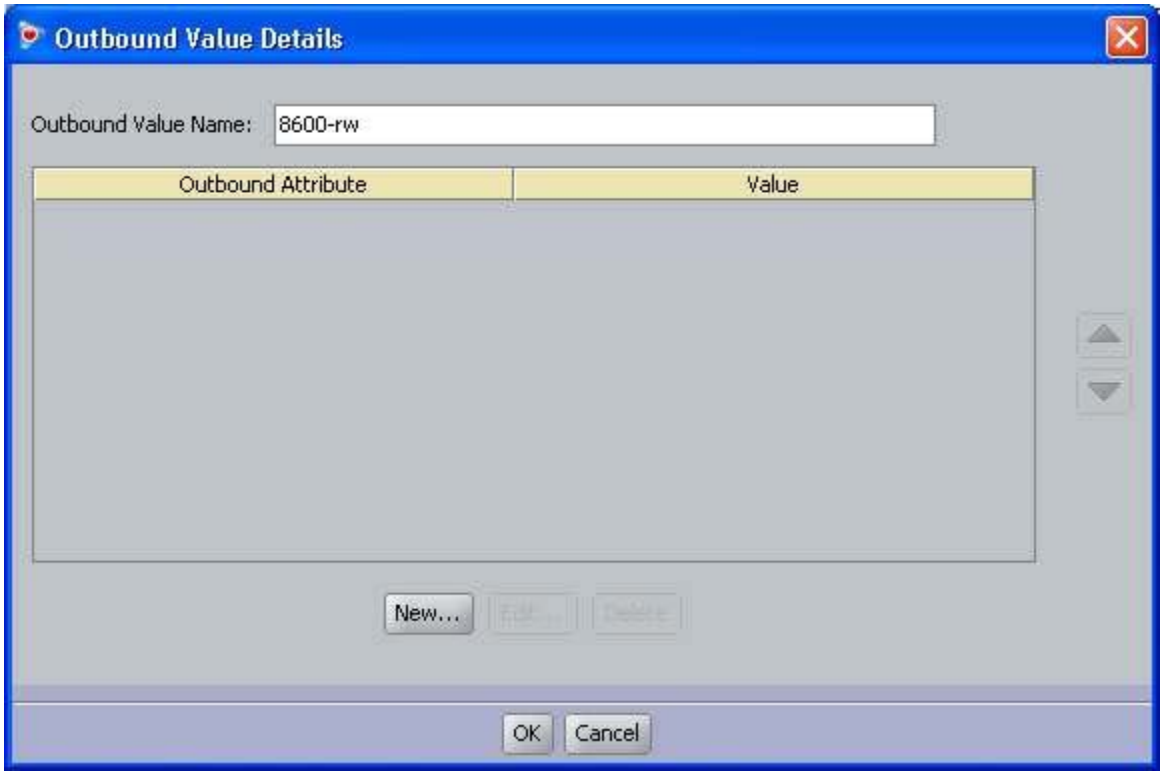
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 6 – Select the Outbound Attributes name created in Step 3 (i.e. ERS8600-Access-Priority as used in this example) via the *Choose Global Outbound Attribute:* pull down menu. In the *Value Unsigned – 32 bit* window, enter 1 (i.e. value of 1 signifies read-only-access). Click on *OK* twice when done.



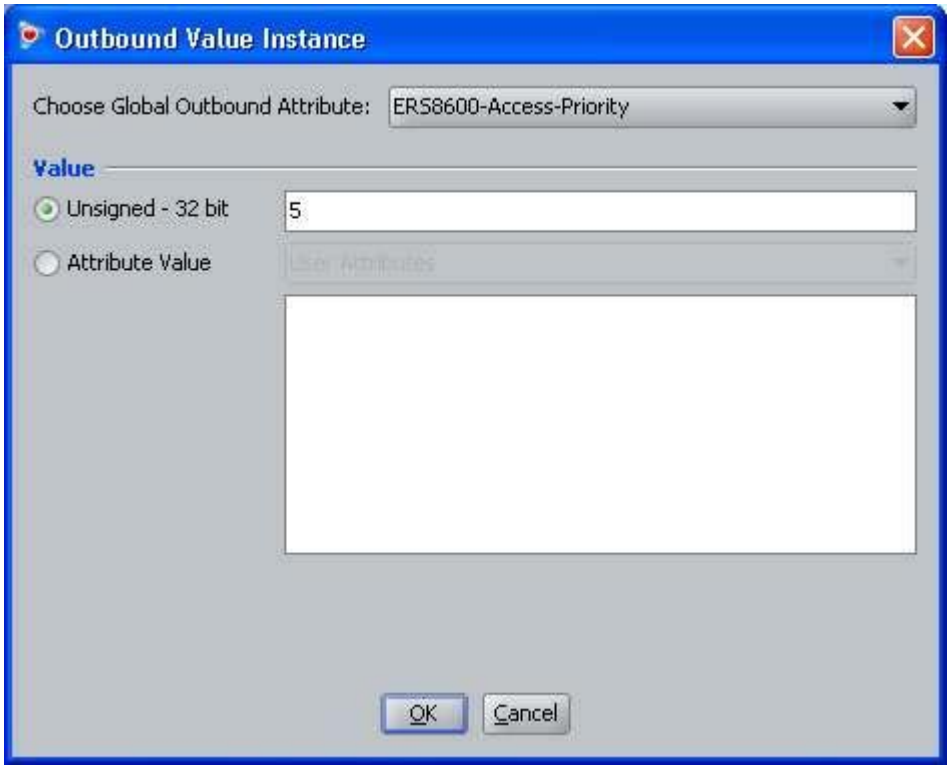
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 7 – Go to *Site Configuration -> Provisioning -> Outbound Values -> New* again to create the outbound attribute for read-write-access. Using the Outbound Attribute created in Step 3, we will add an attribute value of 5 for read-write-access. Start by entering a name via the *Outbound Value Name:* window (i.e. 8600-rw as used in this example) and click on *New*



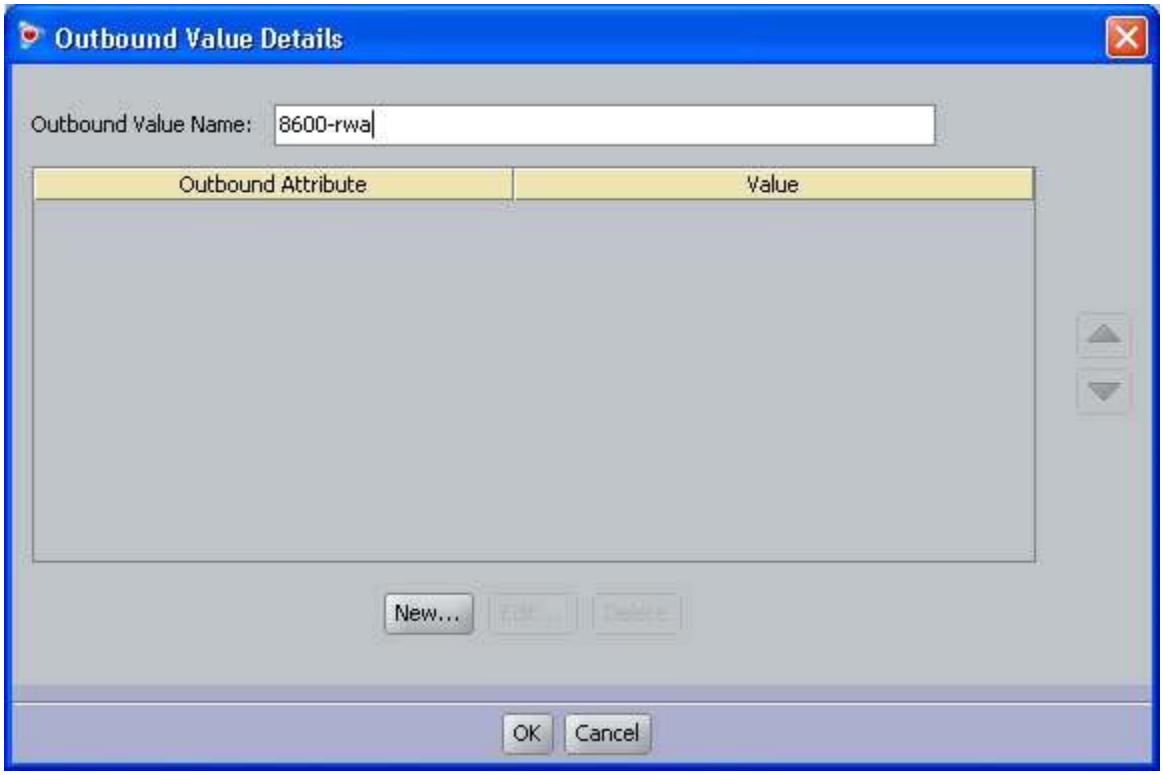
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 8 –Select the Outbound Attributes name created in Step 3 (i.e. ERS8600-Access-Priority as used in this example) via the *Choose Global Outbound Attribute:* pull down menu. In the *Value Unsigned – 32 bit* window, enter 5 (i.e. value of 5 signifies read-write-access). Click on *OK* twice when done.



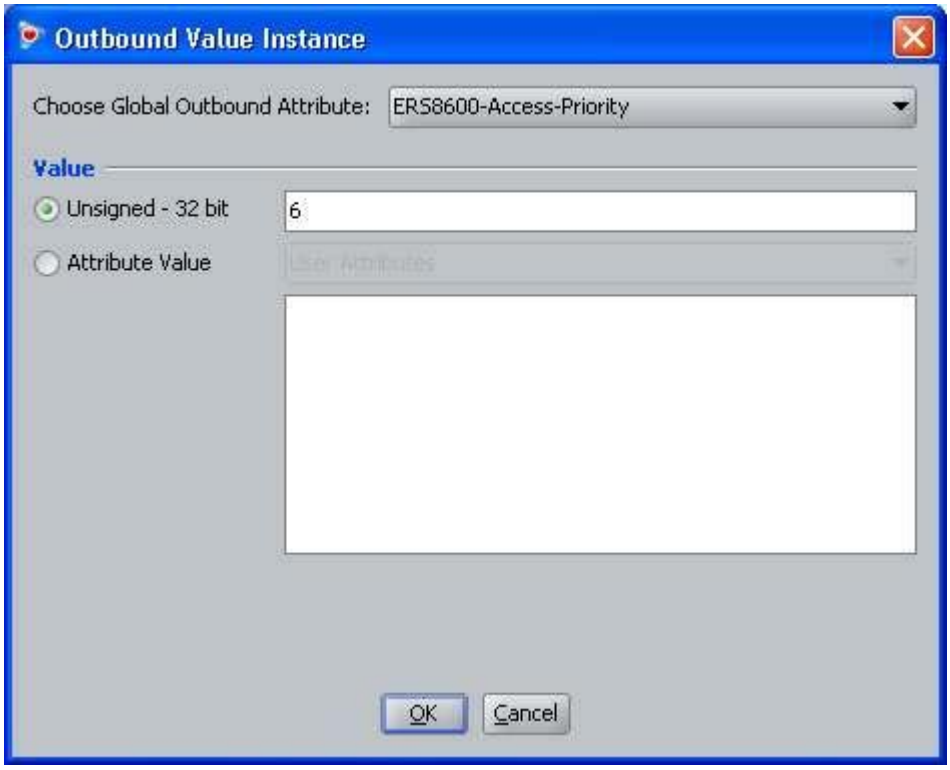
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 9 – Go to *Site Configuration -> Provisioning -> Outbound Values -> New* again to create the outbound attribute for read-write-all-access. Using the Outbound Attribute created in Step 3, we will add an attribute value of 6 for read-write-all-access. Start by entering a name via the *Outbound Value Name:* window (i.e. 8600-rwa as used in this example) and click on *New*



 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 10 –Select the Outbound Attributes name created in Step 3 (i.e. ERS8600-Access-Priority as used in this example) via the *Choose Global Outbound Attribute:* pull down menu. In the *Value Unsigned – 32 bit* window, enter 6 (i.e. value of 6 signifies read-write-all-access). Click on *OK* twice when done.



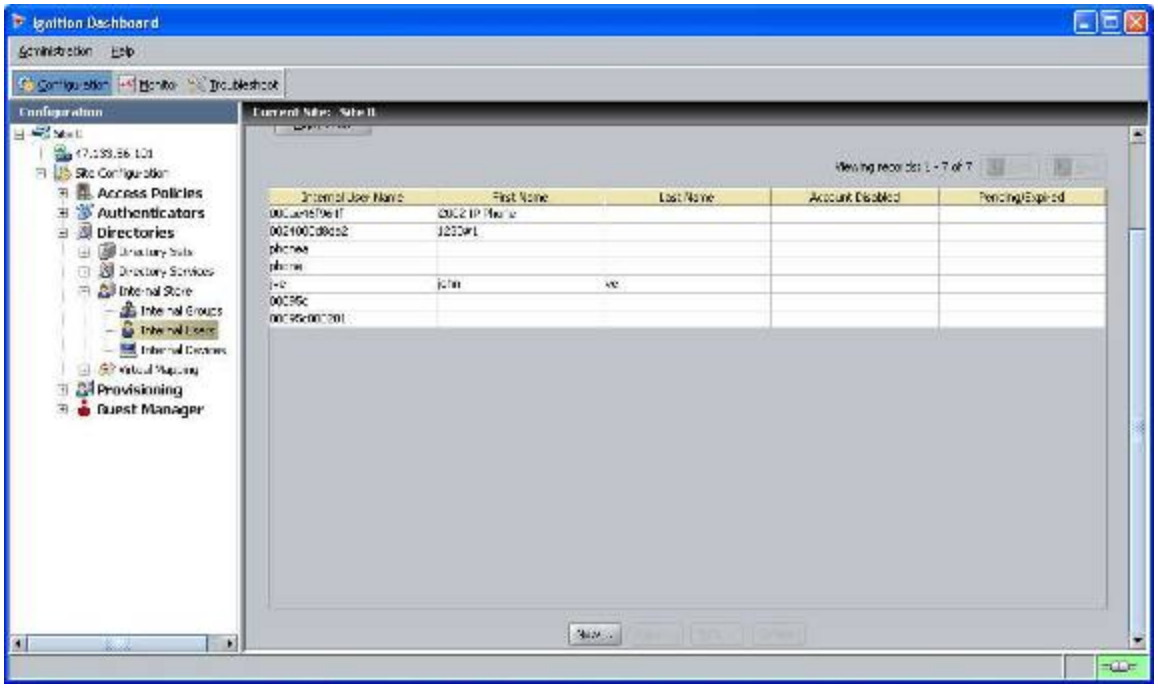
 Copyright © 2009 Nortel Networks. All Rights Reserved.

2.1.3.2 Add Users

For this configuration example, we will add the following users.

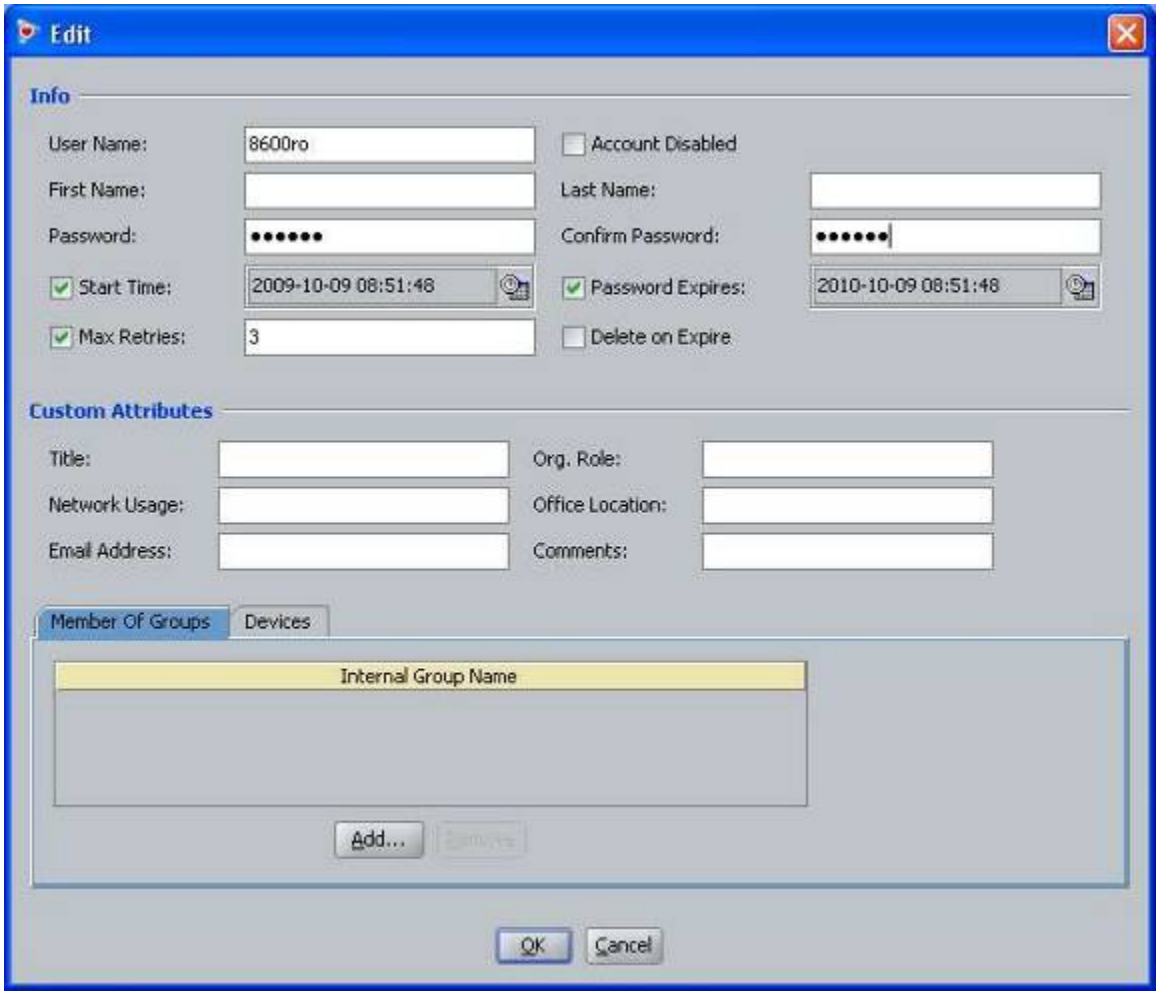
User Name	Access Level
8600ro	Read-Only-Access
8600rw	Read-Write-Access
8600rwa	Read-Write-All-Access

IDE Step 1 – Start by going to *Site Configuration -> Directories -> Internal Store -> Internal Users* and click on *New*



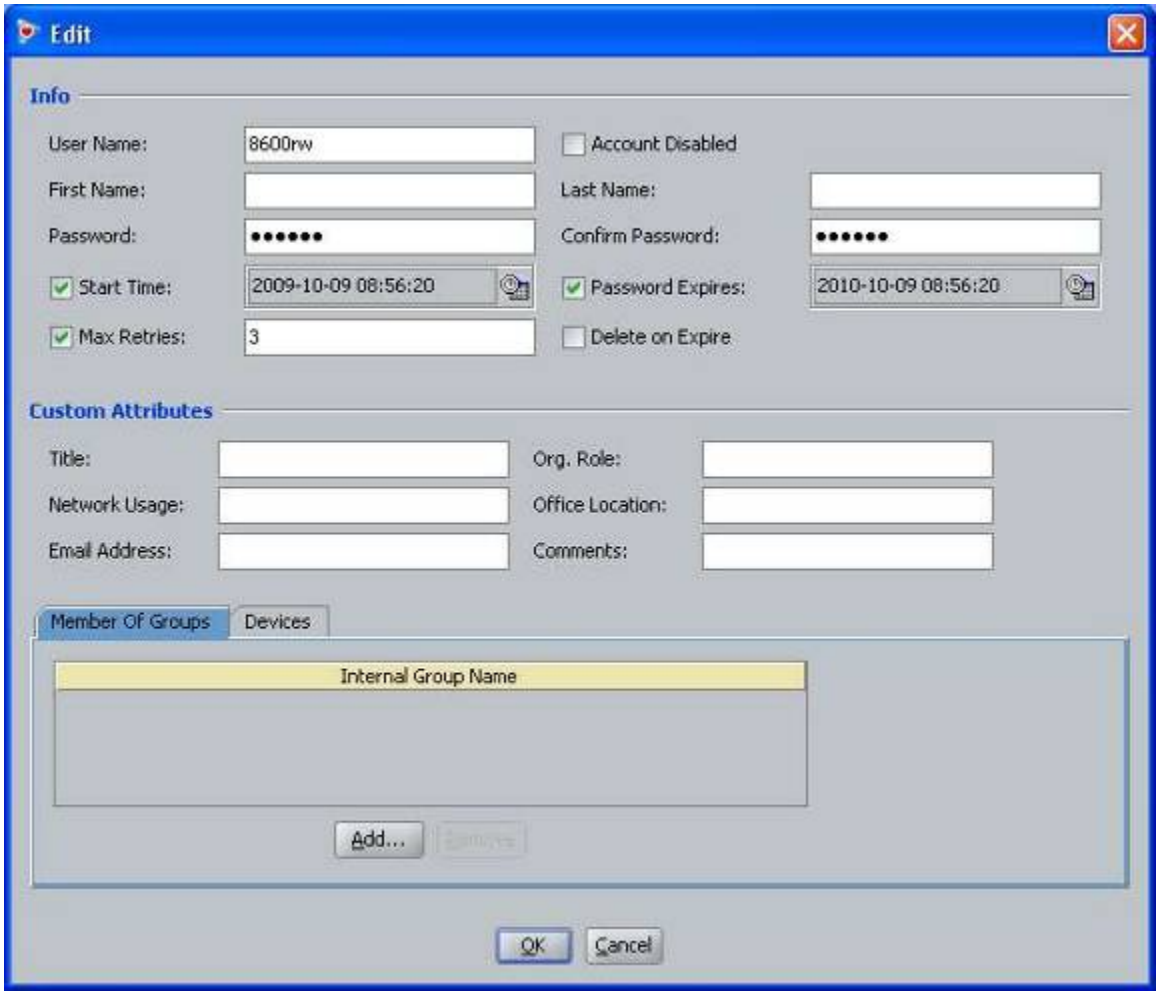
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 2 – Enter the user name for read-only-access via *User Name:* (i.e. 8600ro as used in this example) and enter the password for this user via *Password* and *Confirm Password*. Click on *OK* when done. If you wish, you can also change the expiry date via *Password Expires* if you do not wish to use the default setting of one year



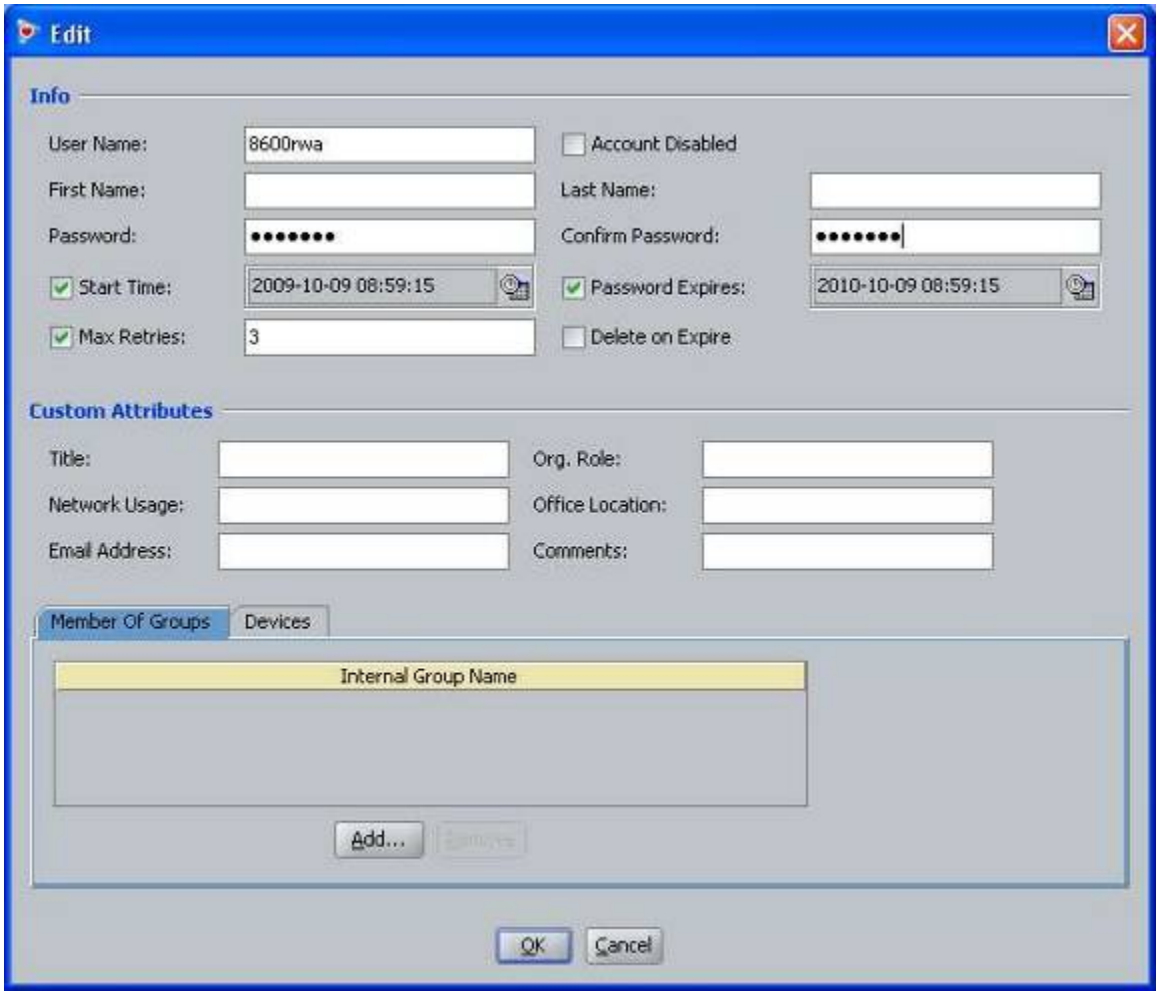
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 3 – Repeat step 2 again by clicking on New to add the read-write-access user. Enter the user name for read-write-access via *User Name:* (i.e. 8600rw as used in this example) and enter the password for this user via *Password* and *Confirm Password*. Click on *OK* when done. If you wish, you can also change the expiry date via *Password Expires* if you do not wish to use the default setting of one year



 Copyright © 2009 Nortel Networks. All Rights Reserved.

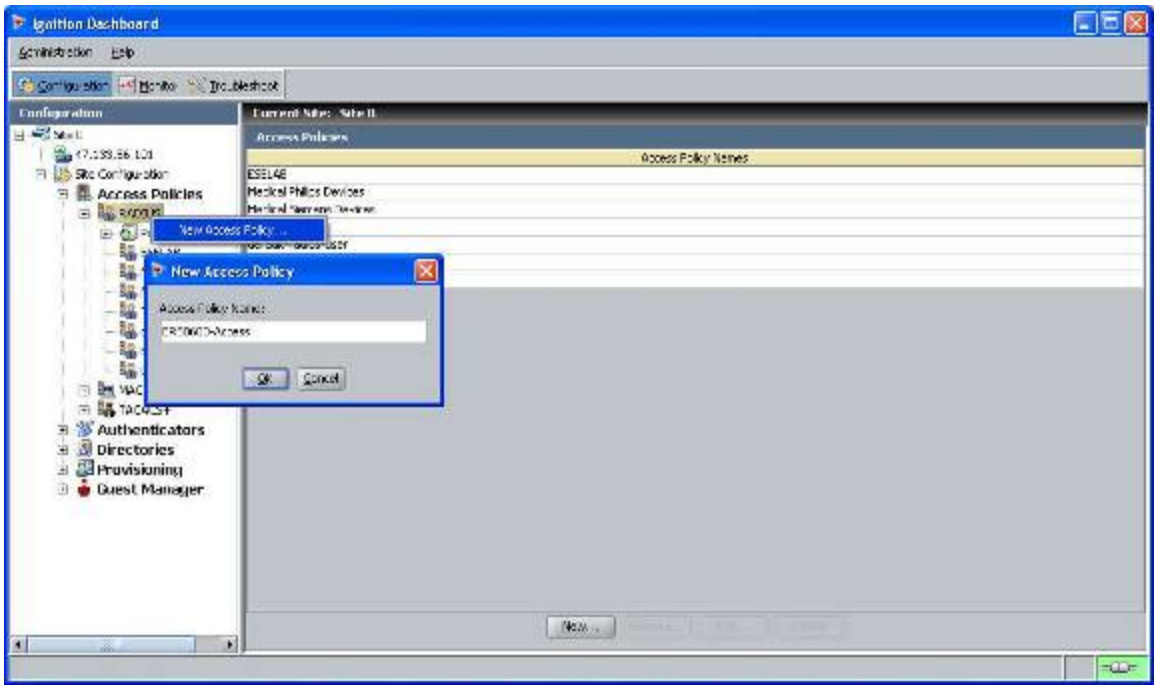
IDE Step 4 – Repeat step 2 for the final time by clicking on New to add the read-write-all-access user. Enter the user name for read-write-all-access via *User Name:* (i.e. 8600rwa as used in this example) and enter the password for this user via *Password* and *Confirm Password*. Click on *OK* when done. If you wish, you can also change the expiry date via *Password Expires* if you do not wish to use the default setting of one year



 Copyright © 2009 Nortel Networks. All Rights Reserved.

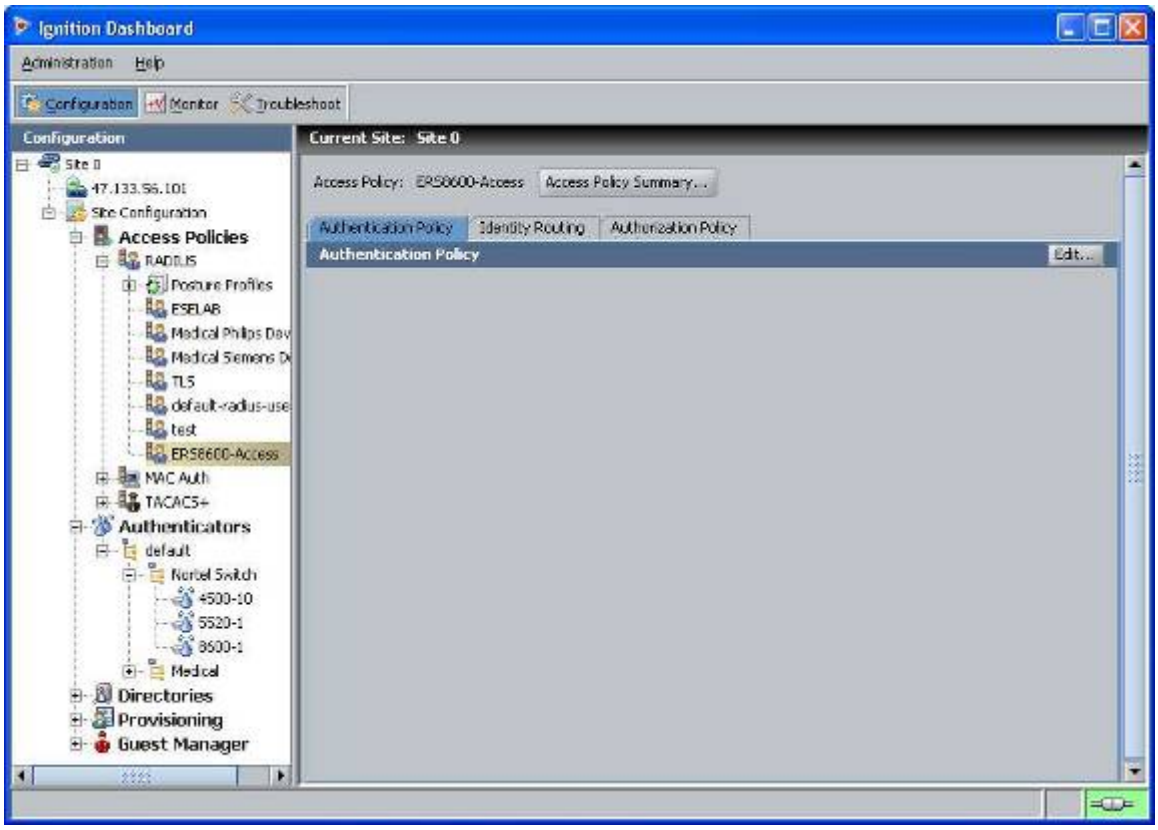
2.1.3.3 Add an Access Policy

IDE Step 1 – Go to *Site Configuration -> Access Policies -> RADIUS.* Right-click R*ADIUS* and select *New Access Policy*. Enter a policy name (i.e. ERS8600-Access as used in this example) and click on *OK* when done



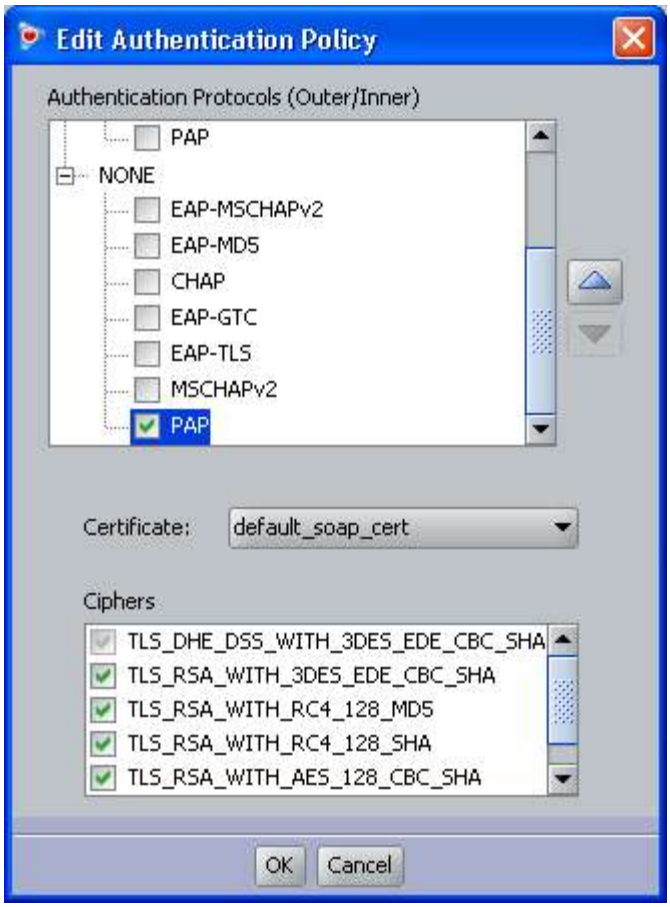
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 2 – Click on the policy we just created, i.e. ERS8600-Access, and click on *Edit* via the *Authentication Policy* tab



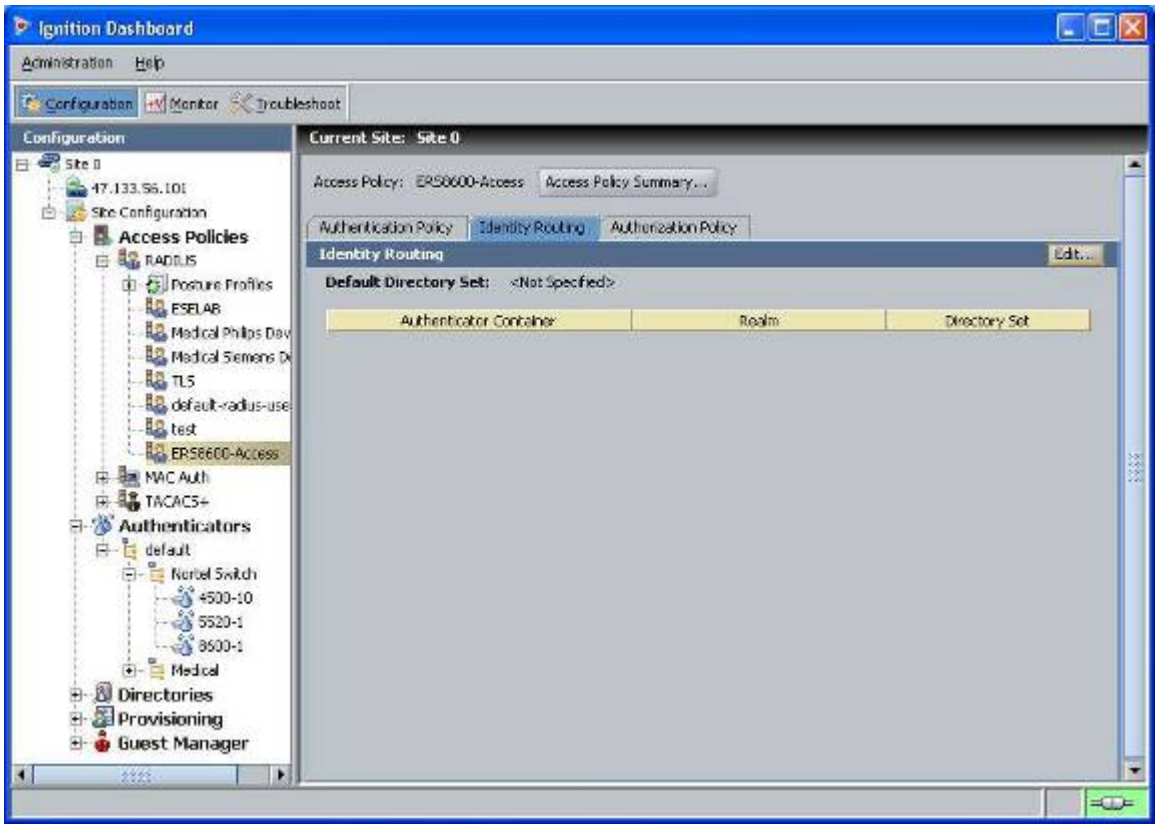
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 3 – Under *Edit Authentication Policy* window, select *NONE -> PAP*



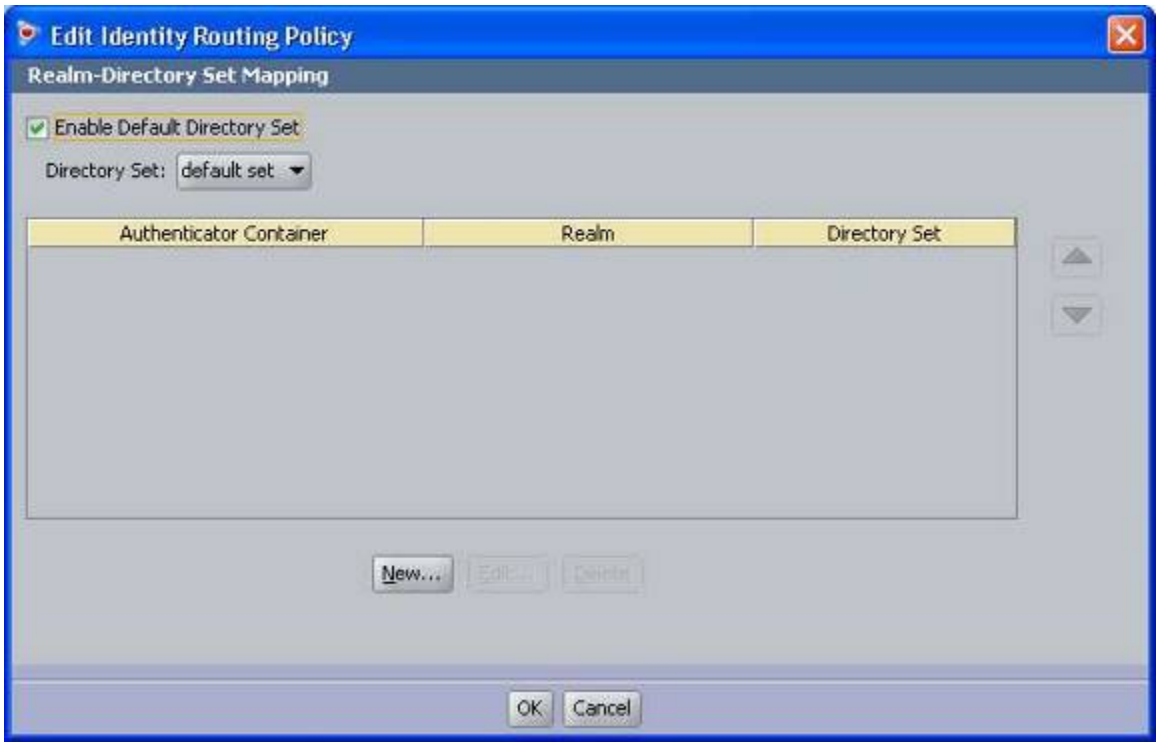
Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

IDE Step 4 – Go to the *Identity Routing tab* and click on *Edit*



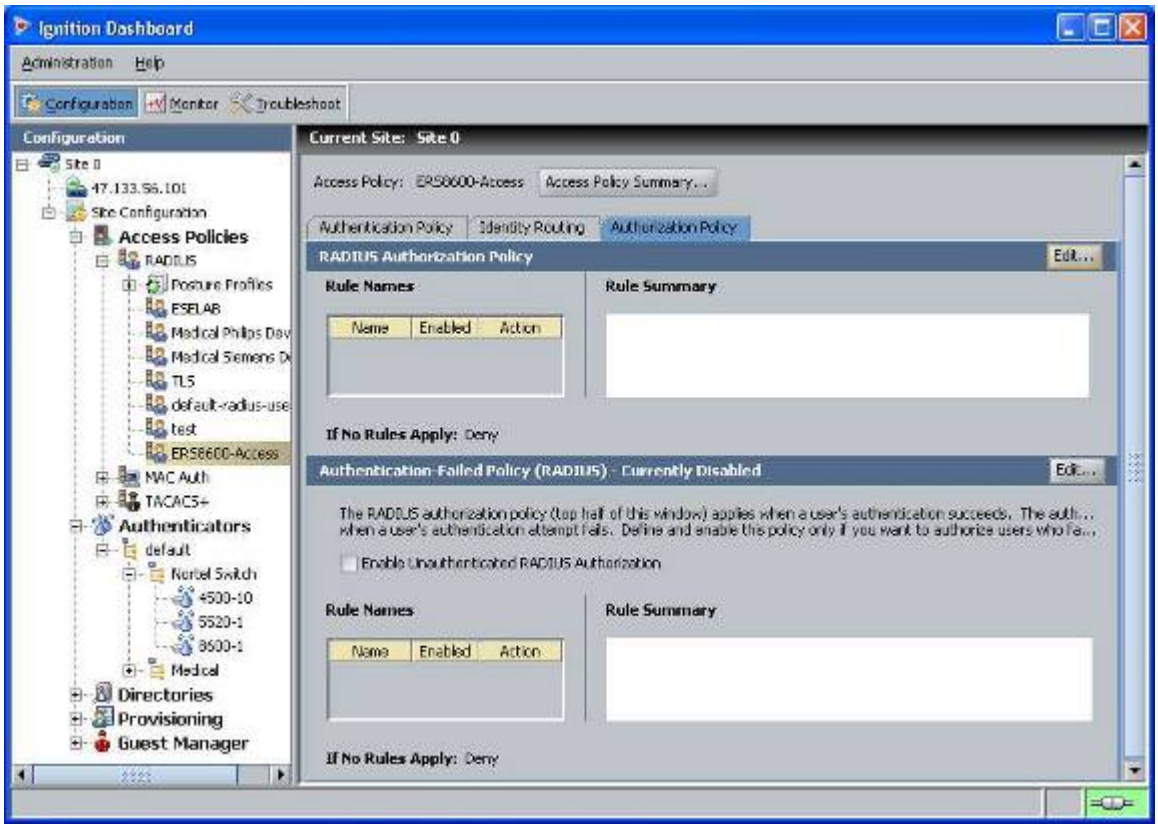
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 5 – Check off the *Enable Default Directory Set* and click on *OK* when done.



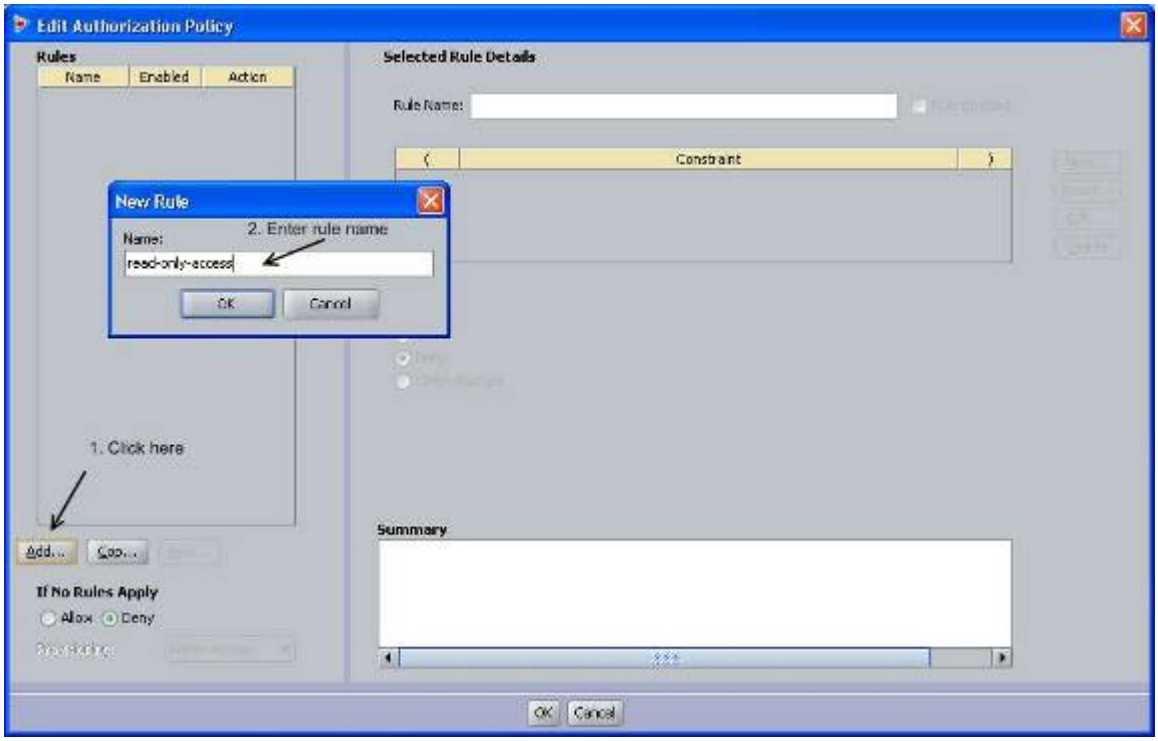
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 6 – Go to the *Authorization Policy* tab and click on *Edit*



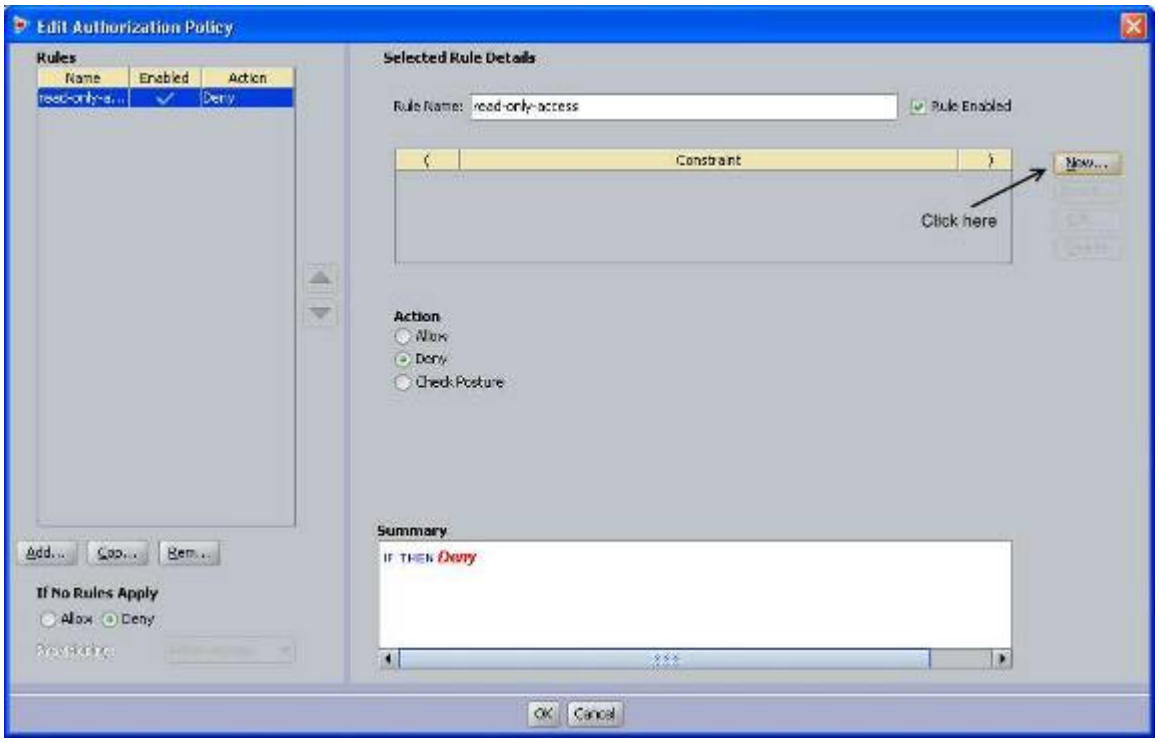
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 7 – Once the *Edit Authorization Policy* window pops up, click on *Add.* First, we will add a rule for read-only-access. When the *New Rule* window pops up, we will name the rule *read-only-access* as shown below



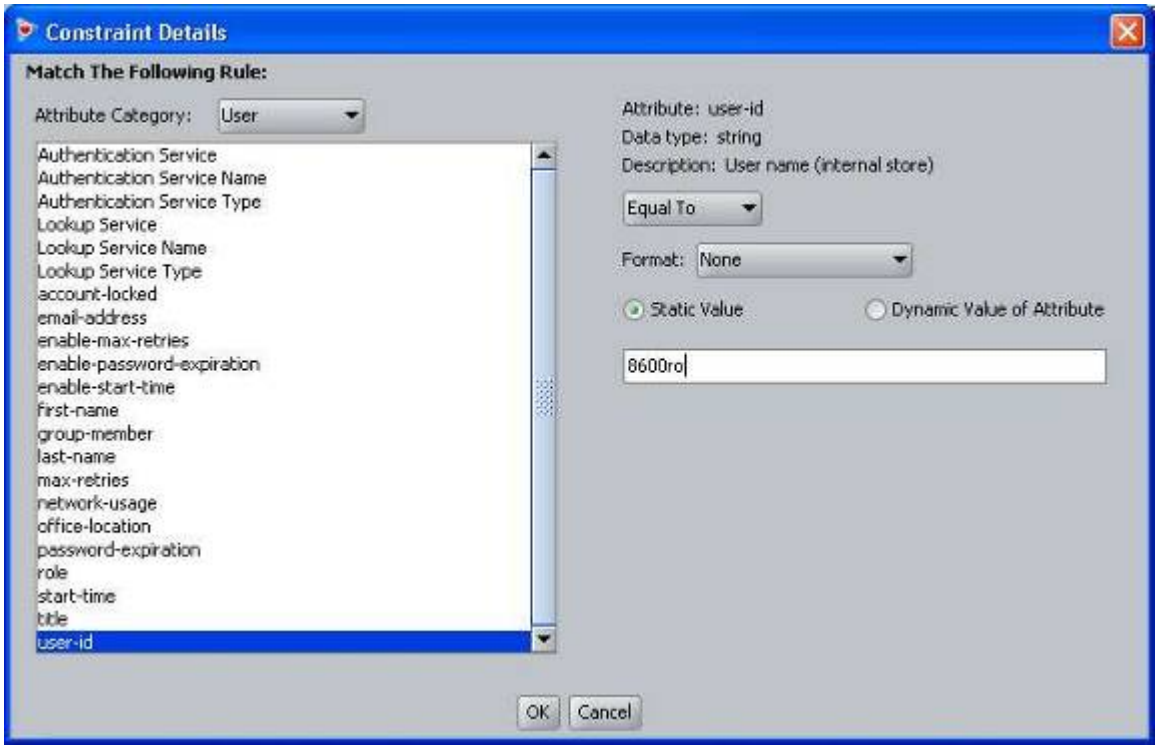
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 8 – Click on *New* to add a new constraint



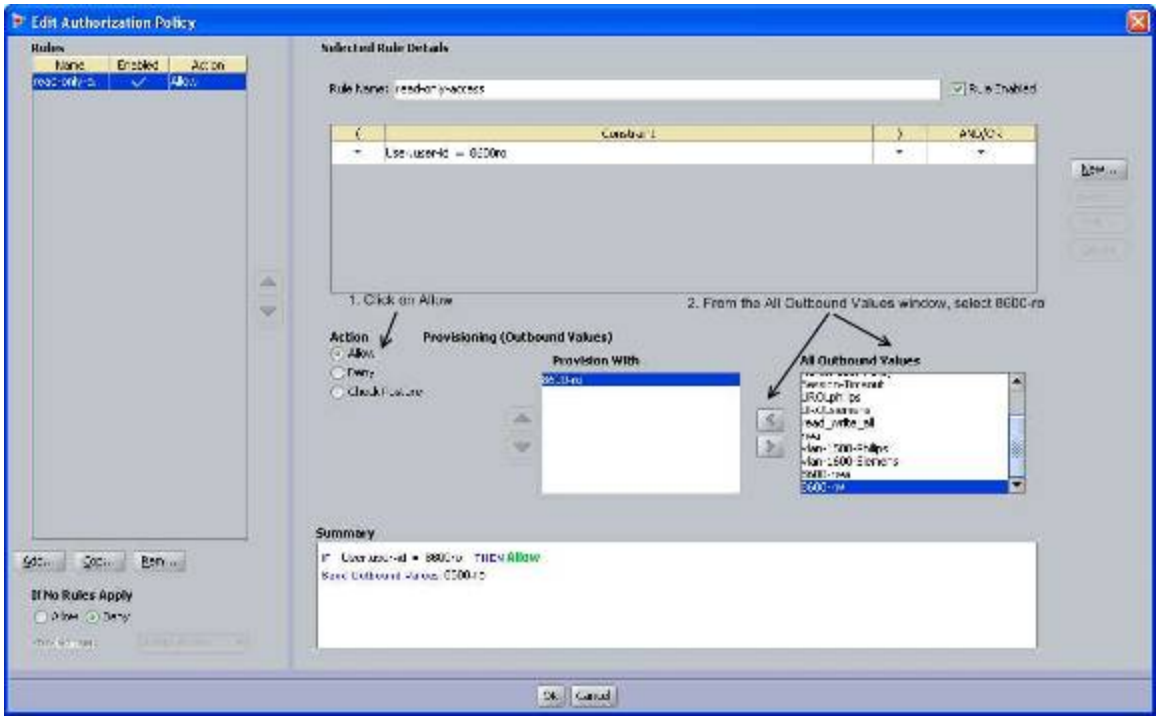
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 9 – For this example, we are simply going to look for the read-only-user user-id. From *Attribute Category*, select *User* and scroll down and select *user-id*. Select *Equal To* with *Format* of *None* and enter the read-only-access user id, i.e. 8600ro as used in this example, in the *Static Value* window as shown below. Click on *OK* when done



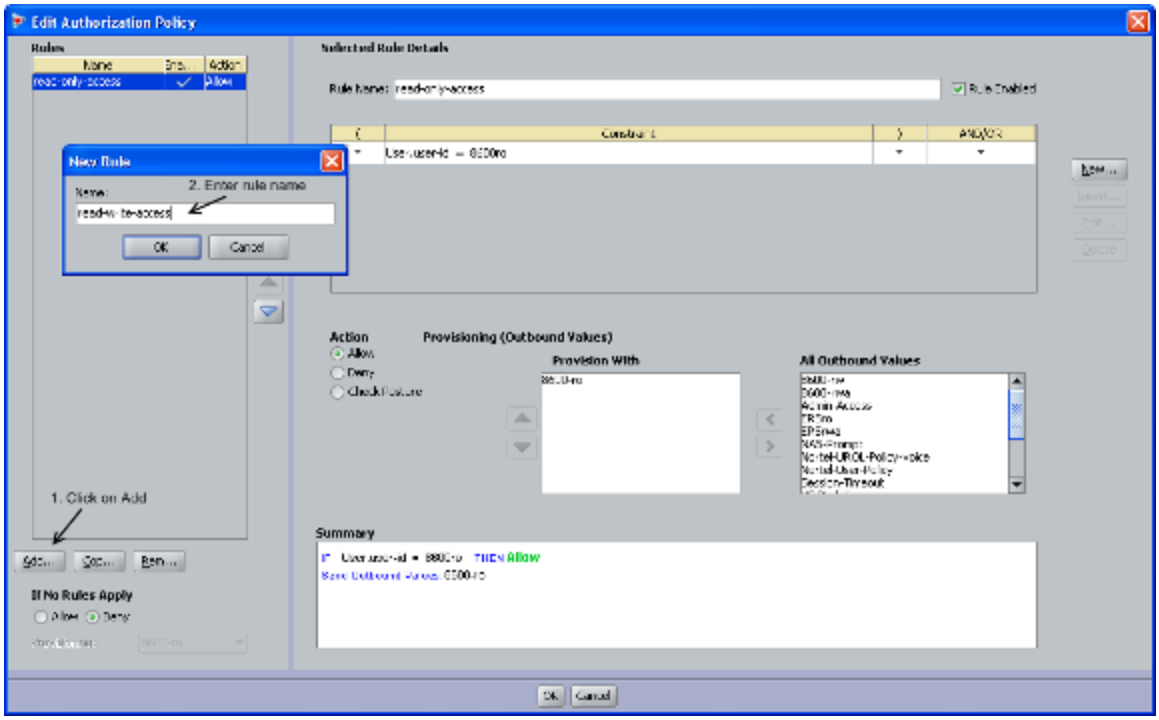
Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

IDE Step 10 – Via *Actions*, select *Allow*. From the *All Outbound Values* window, select the output attribute we created previously named *8600ro* and click on the less-than arrow key to move the attribute to the *Provision With* window



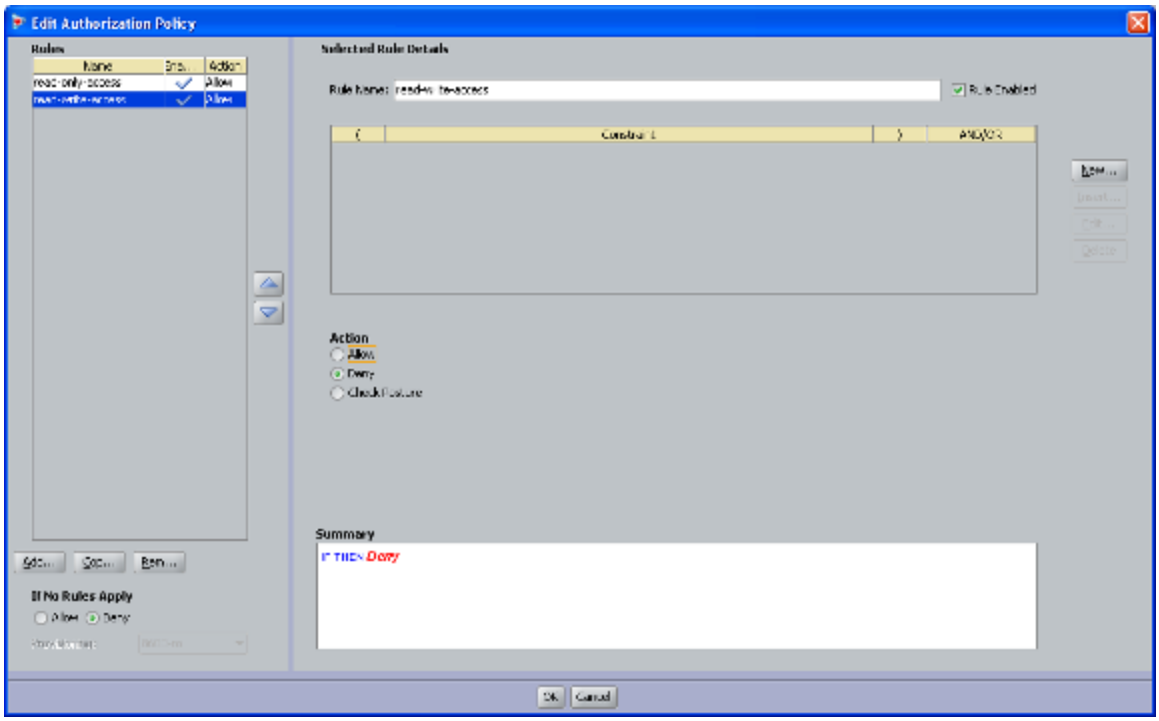
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 11 – Next, we will add a rule for read-write-access. Start by clicking on *Add* and when the *New Rule* window pops up, add an appropriate name for this rule, i.e. read-write-access as used in this example



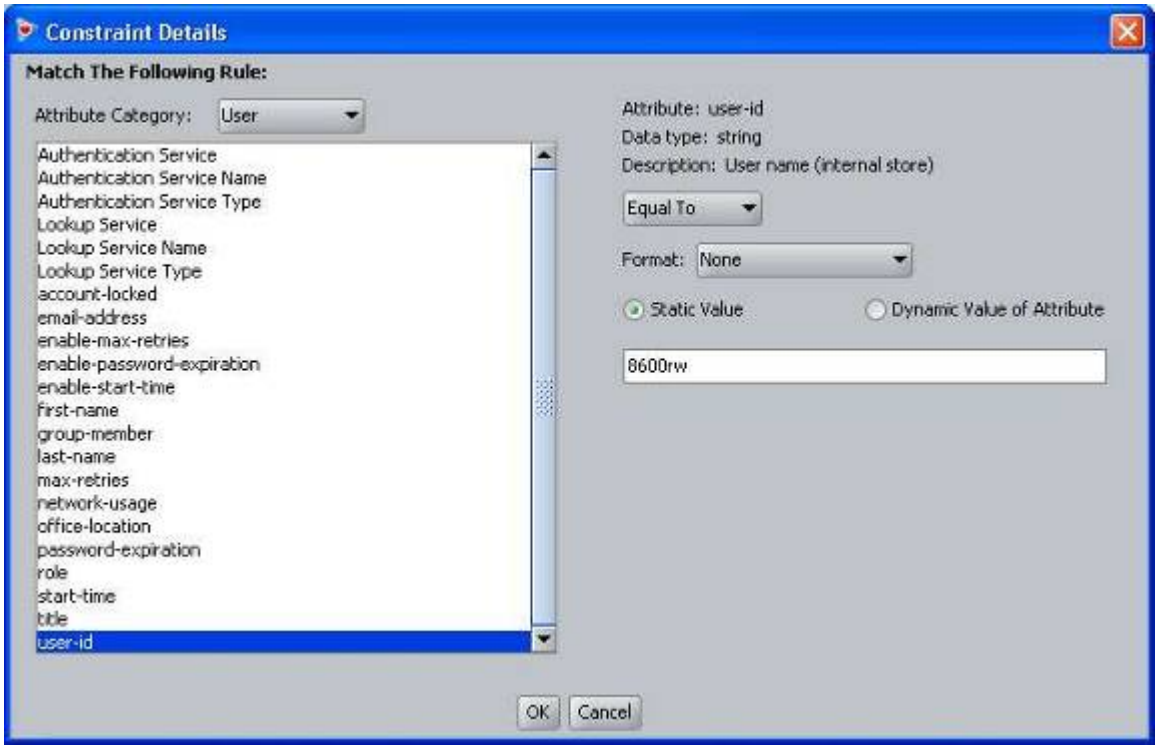
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 12 – Click on *New* to add a new constraint



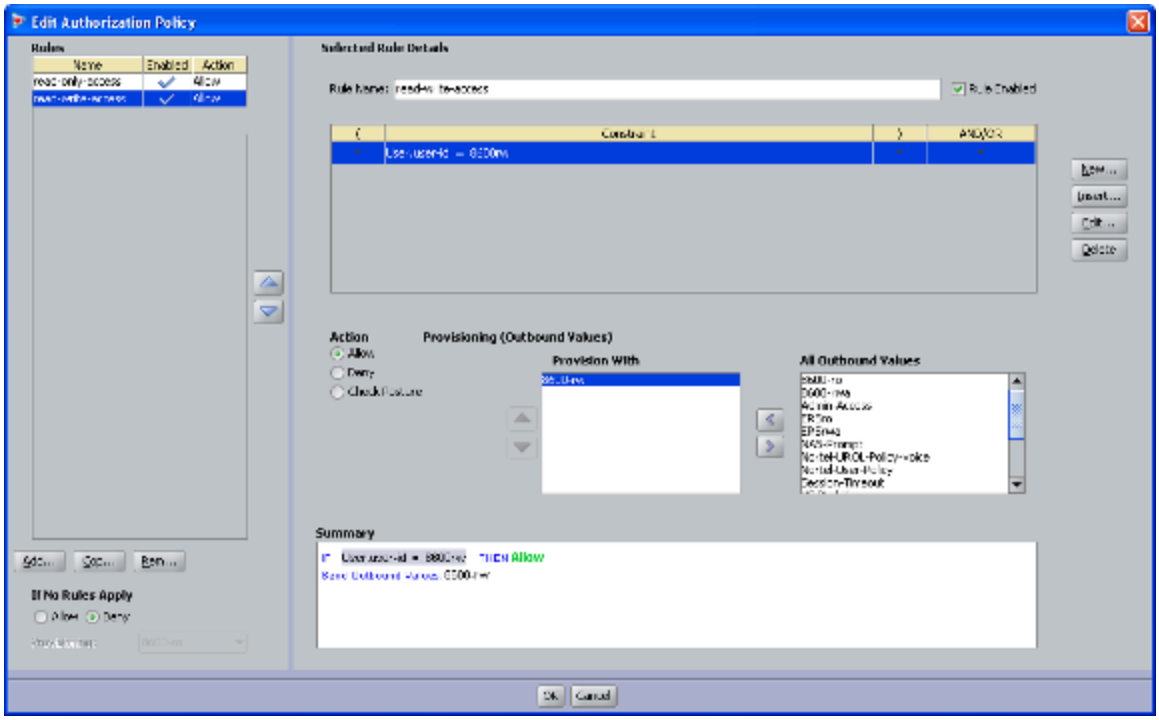
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 13 – For this example, we are simply going to look for the read-write-access user-id. From *Attribute Category*, select *User* and scroll down and select *user-id*. Select *Equal To* with *Format* of *None* and enter the read-only-access user id, i.e. *8600rw* as used in this example, in the *Static Value* window as shown below. Click on *OK* when done



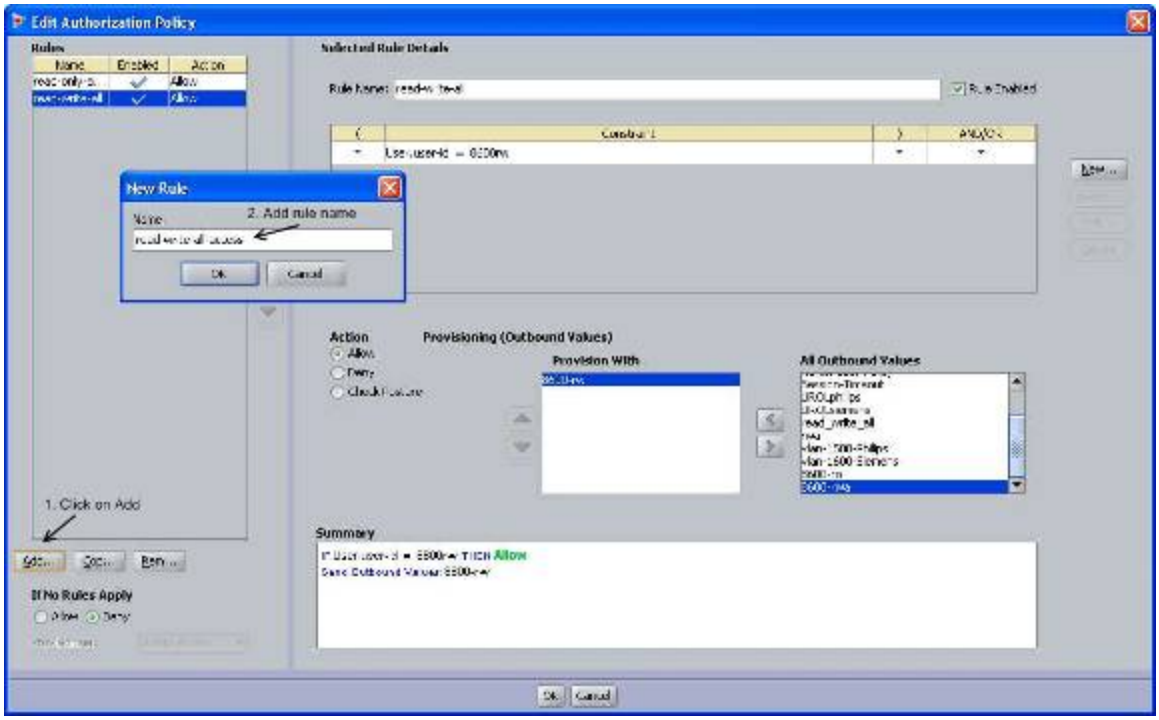
Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

IDE Step 14 – Via *Action*, select *Allow*. From the *All Outbound Values* window, select the output attribute we created previously named *8600rw* and click on the less-than arrow key to move the attribute to the *Provision With* window



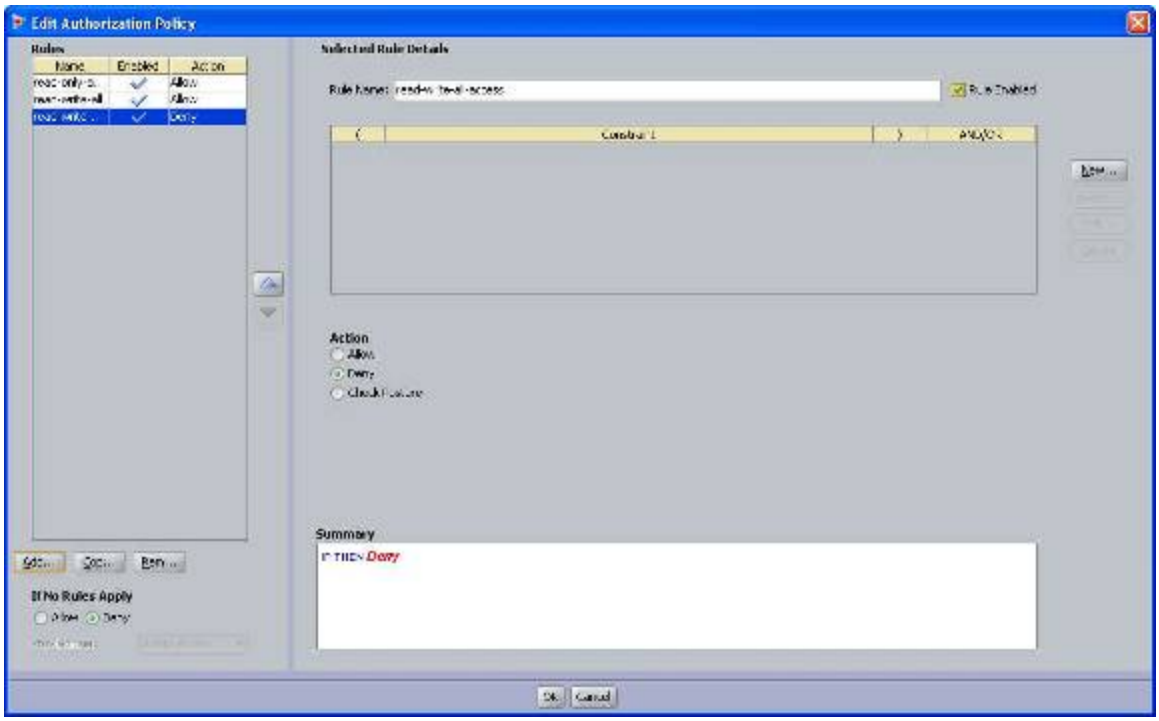
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 15 – Finally, we will add a rule for read-write-all-access. Start by clicking on *Add* and when the *New Rule* window pops up, add an appropriate name for this rule, i.e. *read-write-all-access* as used in this example



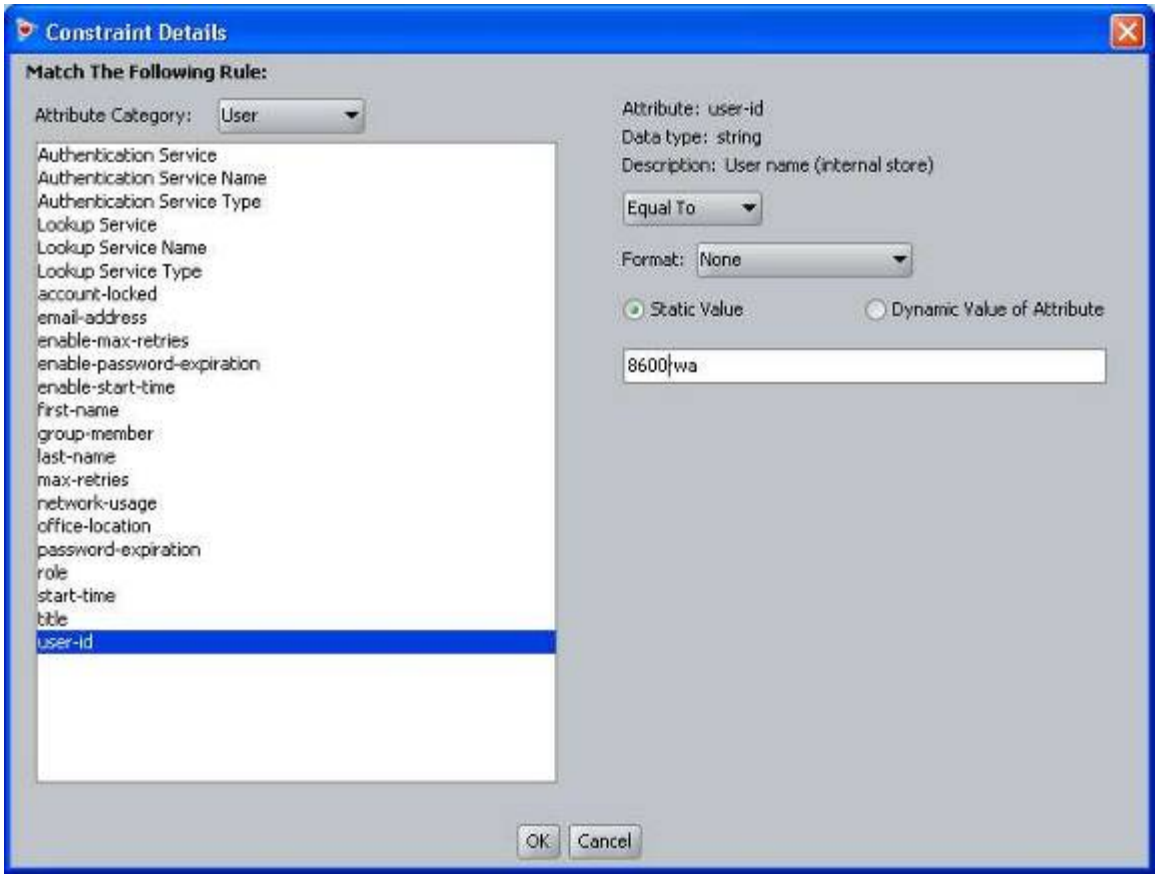
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 16 – Click on *New* to add a new constraint



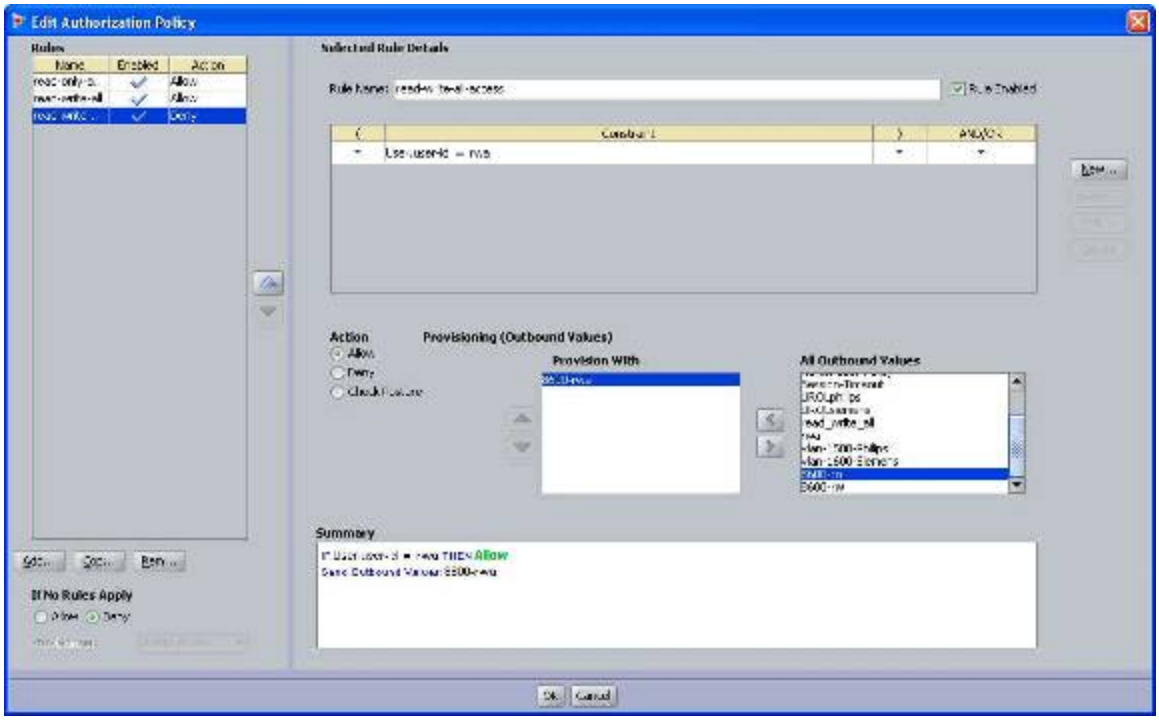
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 17 – For this example, we are simply going to look for the read-write-all-access user-id. From *Attribute Category*, select *User* and scroll down and select *user-id*. Select *Equal To* with *Format* of *None* and enter the read-only-access user id, i.e. *8600rwa* as used in this example, in the *Static Value* window as shown below. Click on *OK* when done



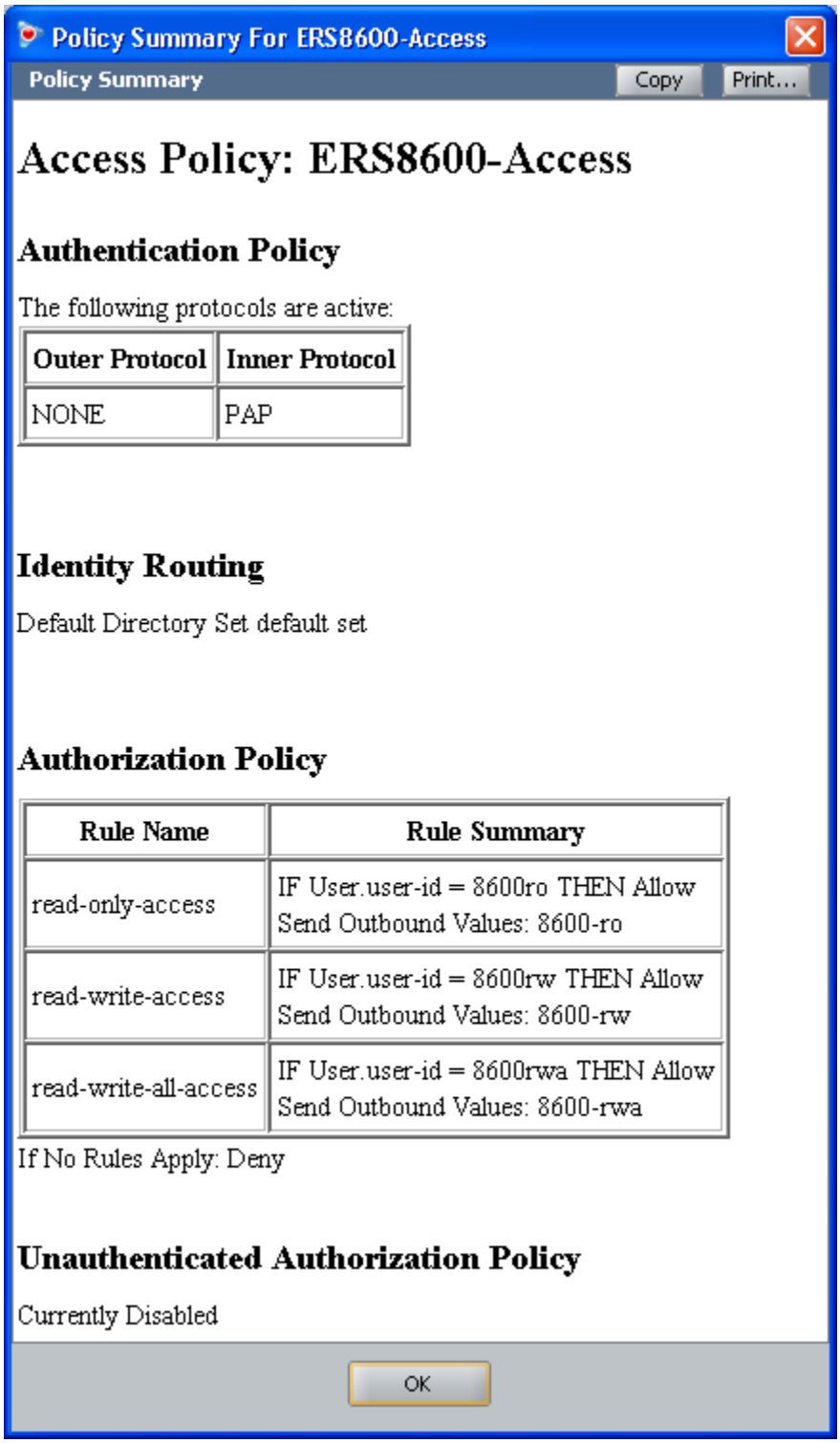
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 18 – Via *Action*, select *Allow*. From the *All Outbound Values* window, select the output attribute we created above named *8600rwa* and click on the less-than arrow key to move the attribute to the *Provision With* window



 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 19 – When completed, you can view the complete policy by clicking on the *Access Policy Summary* button

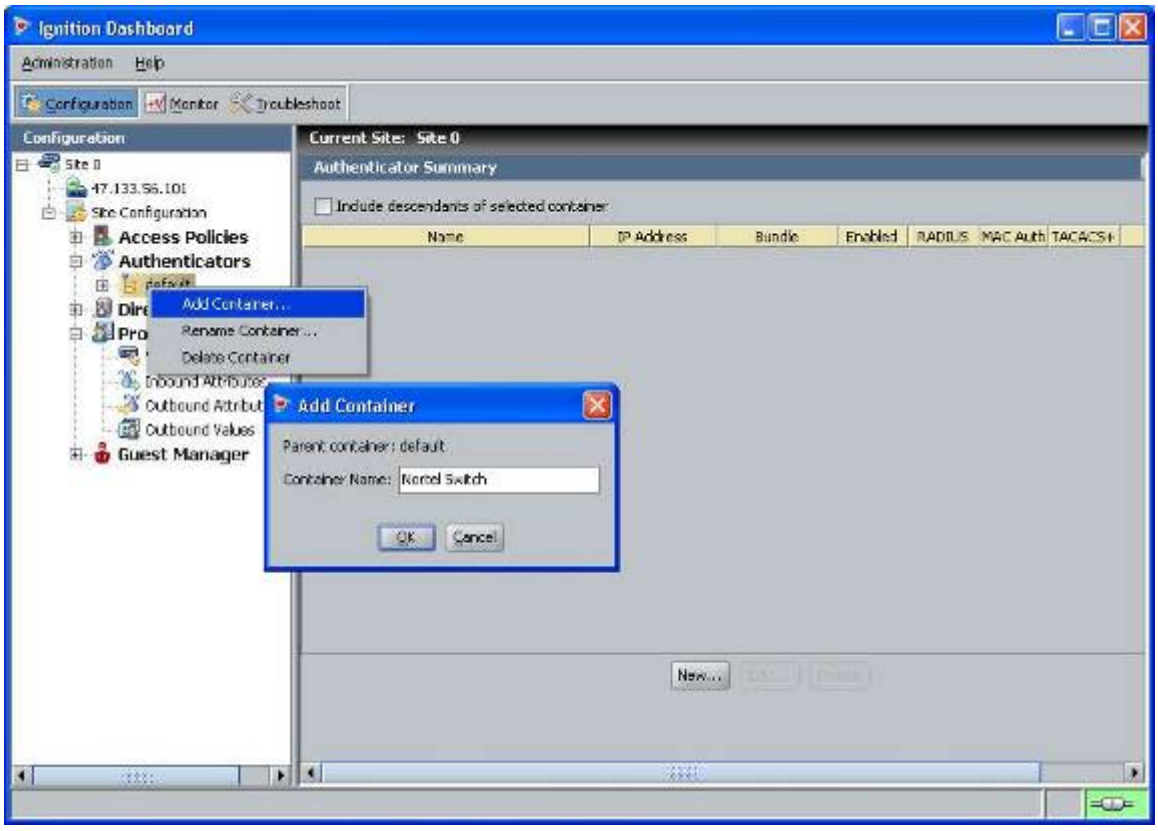


 Copyright © 2009 Nortel Networks. All Rights Reserved.

2.1.3.4 Add the Nortel ERS8600-1 switch as an RADIUS Authenticator

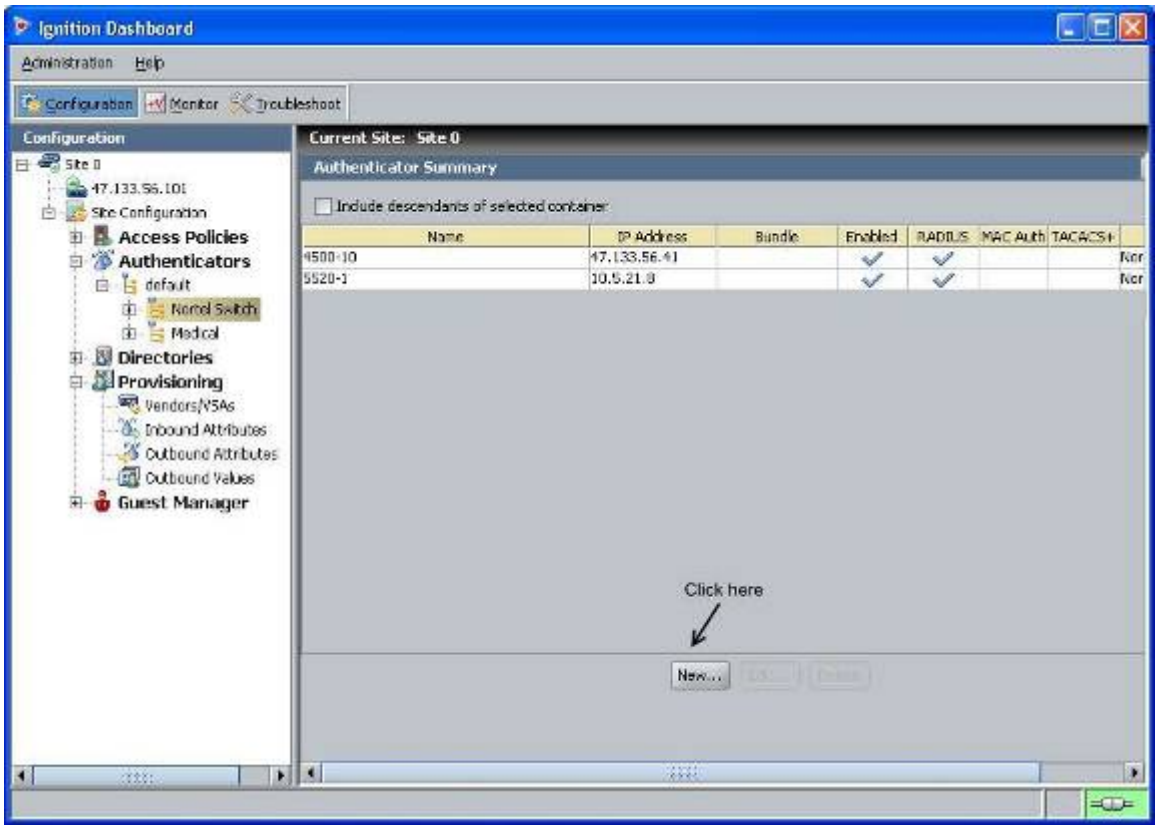
For Ignition Server to process the Nortel switch RADIUS requests, each switch must be added as an Authenticator.

IDE Step 1 – Go to *Site Configuration -> Authenticators -> default.* For this example, we will create new container named *Nortel Switch* by right clicking *default* and selecting *Add Container*



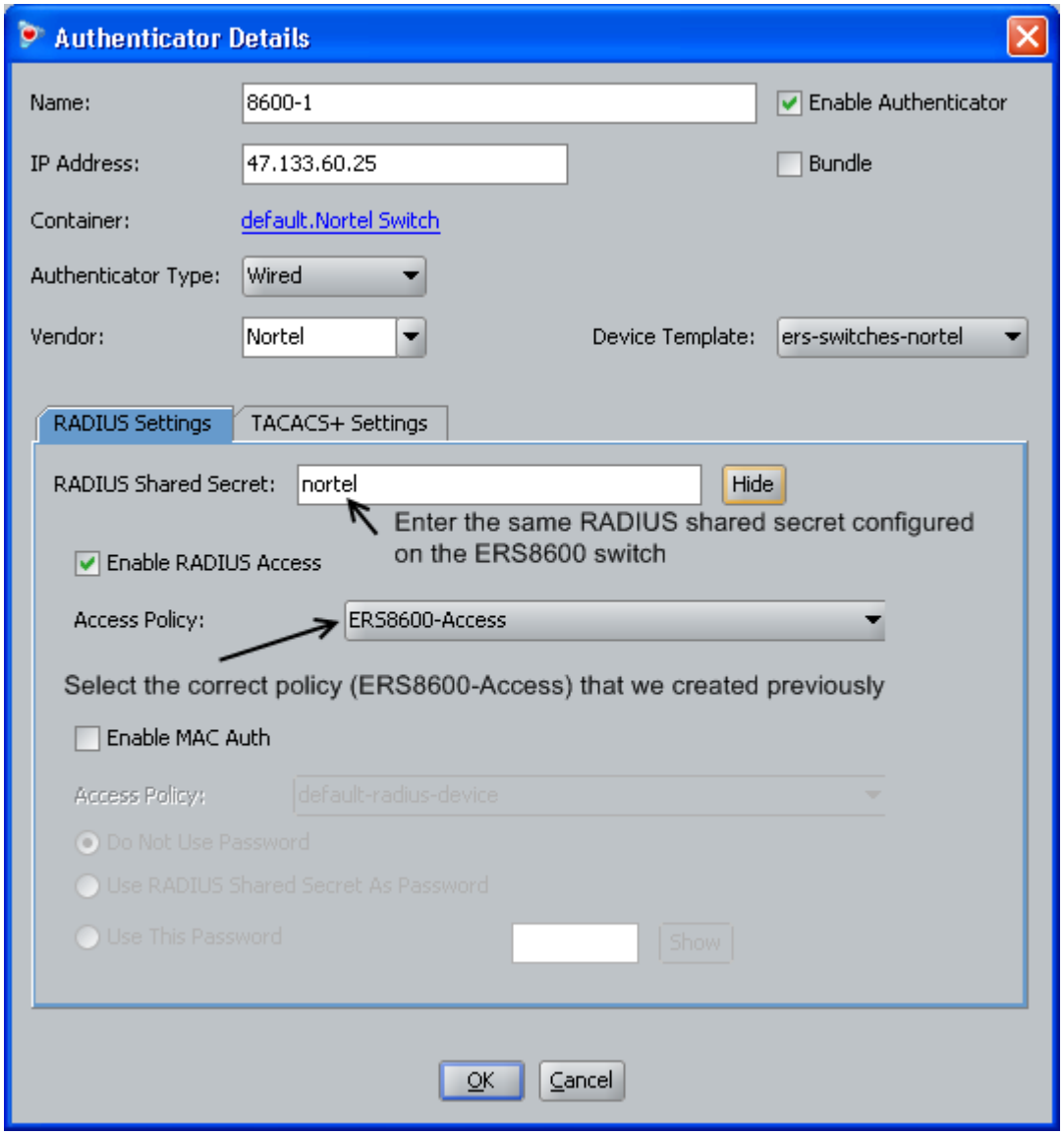
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 2 – Go to *Site Configuration -> Authenticators -> default -> Nortel Switch* and click on *New.*



 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 3 – Enter the settings as shown below making sure you select the policy we created previously named *ERS8600-Access* via *Access Policy*. Leave *Enable Authenticator* and *Enable RADIUS Access* checked. Click on *OK* when done.



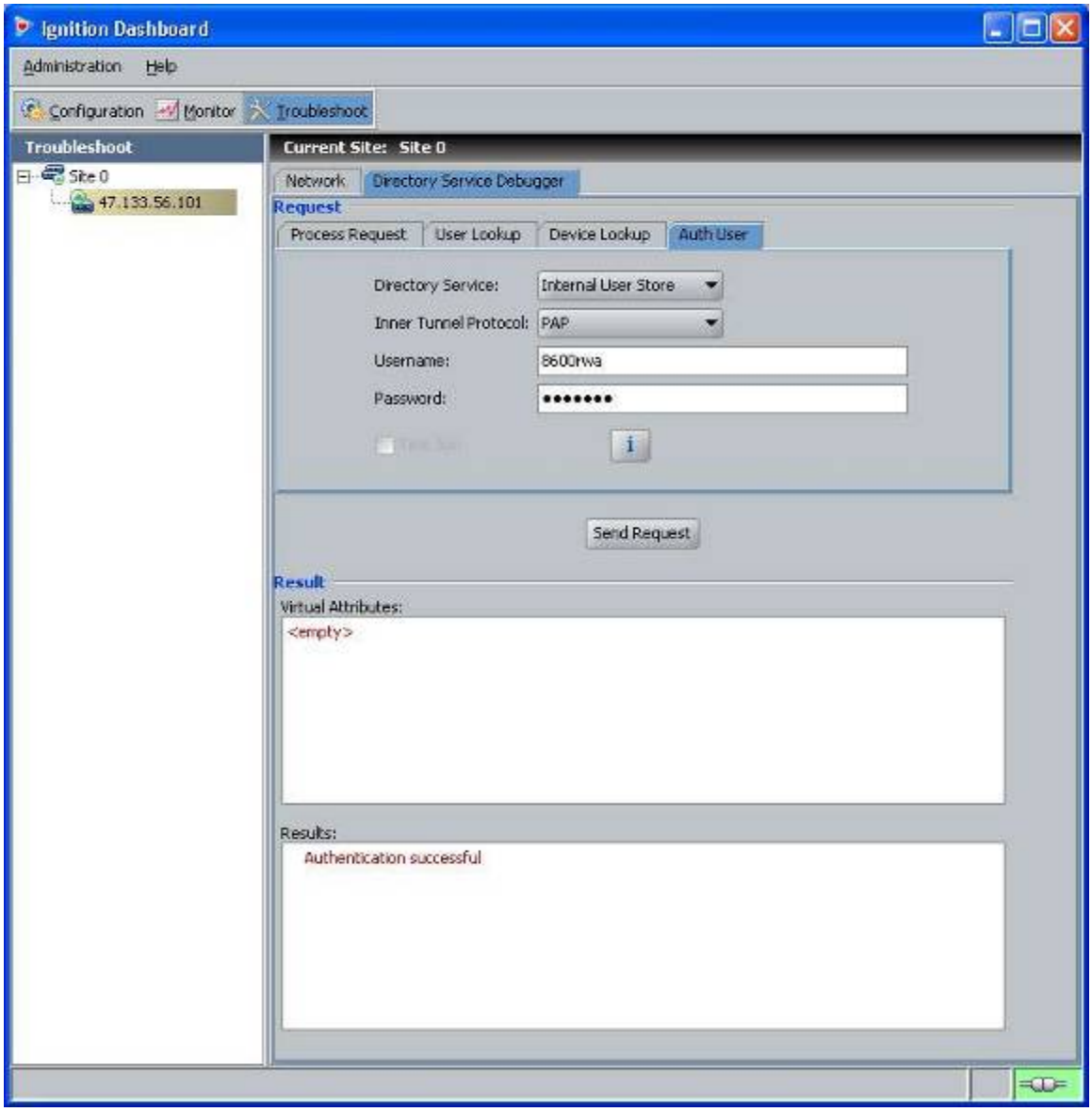
 Copyright © 2009 Nortel Networks. All Rights Reserved.

2.1.4 Verification

2.1.4.1 Verify User Authentication

You can test user authentication for the ERS8600 users configured on IDE by entering the user name and password.

Step 1 – Via Ignition Dashboard, select the IP address of the Ignition Server, click on the *Troubleshoot* tab, go to *Directory Service Debugger* and select the *Auth User* tab. Make you select *Internal User Store* and *PAP* and the enter a valid user name and password configured for the ERS8600 and click on *Send Request.* For more details, repeat the same steps but via the *Process Request* tab instead



 Copyright © 2009 Nortel Networks. All Rights Reserved.

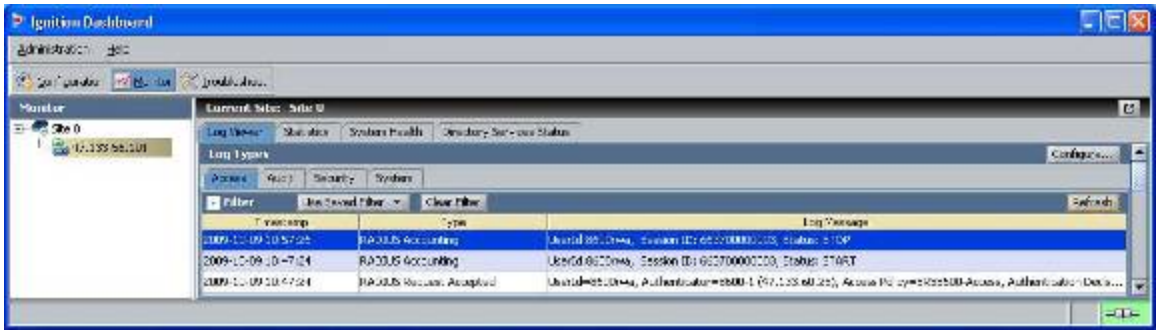
Via Dashboard, verify the following information:

Option	Verify
Results	If successful, ***Authentication successful*** should be displayed

2.1.4.2 Verify user authentication from ERS switch

You can view the authentication details via Ignition Dashboard which provides extensive details about the device or user.

Step 1 – In Dashboard, select the IP address of the Ignition Server and click on the *Monitor* tab, go to *Log Viewer,* and select the *Access* tab. Via the message of a valid user, right-click the message and select *Access Record Details*. Shown before are the results for the read-write-all-access user. Please note you should also see RADIUS accounting records upon a user logging onto and disconnecting from the ERS8600



Result:

 Copyright © 2009 Nortel Networks. All Rights Reserved.

Rights Reserved.

At minimum, verify the following items:

Option	Verify
Authentication Result	If successful, ***Authenticated*** should be displayed. If not, verify the device using the previous step and if this also fails, verify the Ignition Server configuration.
Authorization Result	If successful, ***Allow*** should be displayed. If not, verify the device using the previous step and if this also fails, verify the Ignition Server configuration.
User-Name	Displays the name of the user id, in this example, a user id of ***8600rwa*** was used for the user with read-write-all-access rights.
Access Policy	This field displays the Ignition Server policy used for this user which should be ***ERS8600-Acess*** as configured for this example.
Policy Rule Used Outbound Attribute	For this user, the Policy rule ***read-write-all-access*** as configured above should be used which sends an outbound vendor specific attribute value of ***6*** to the ERS8600 telling the switch this user has read-write-all-access

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.

External Distribution

2.2 Part 2: ERS8600 Configuration with Specific Commands Disabled

In this part, we will use the same configuration used in the previous example, but, we will restrict the read-write ERS8600 user (user name = 8600rw) to deny access to the CLI QoS and Filter configuration (“config qos” or “config filter”).

2.2.1 ERS8600 Configuration

Enable the user access profile parameter on the ERS8600.

ERS8600-1 Step 1 – Enable the RADIUS cli-profile by setting the value to true
ERS-8606:5# ***config radius cli-profile-enable true***

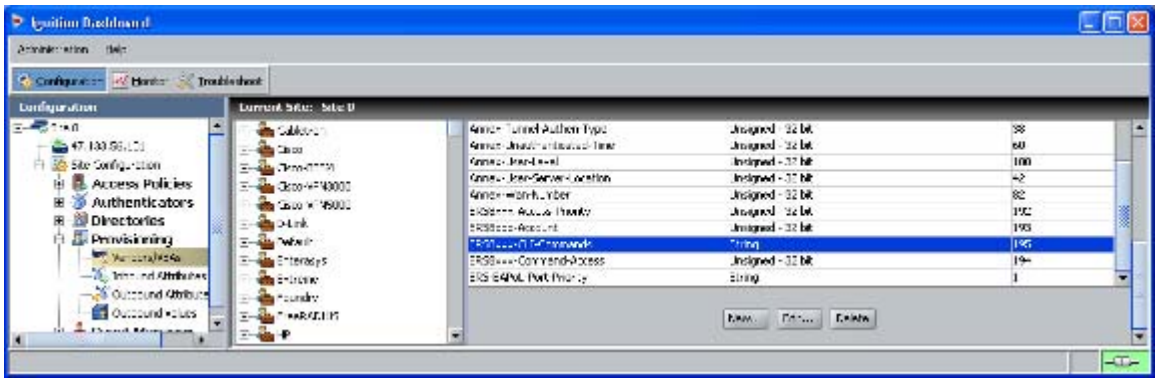
Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

2.2.2 IDE Setup

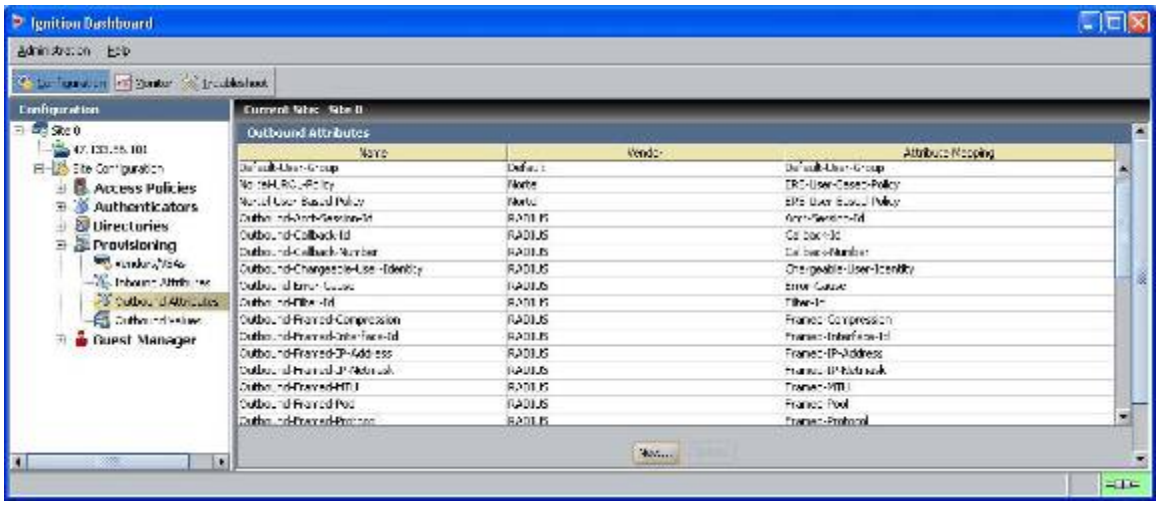
2.2.2.1 Configure Outbound attributes to deny ERS8600 CLI commands

Using the same base configuration from the previous step, we will simple add the CLI commands we wish to deny to the read-write user. In this example, this will apply only to the user *8600rw*.

IDE Step 1 – IDE already has the vendor specific attributes defined, Bay Networks vendor code 1584 using attribute types 194 and 195 for the ERS8600 which can be viewed by going to *Site Configuration -> Provisioning -> Vendors/VSAs -> Bay-Networks -> VSA Definitions.*

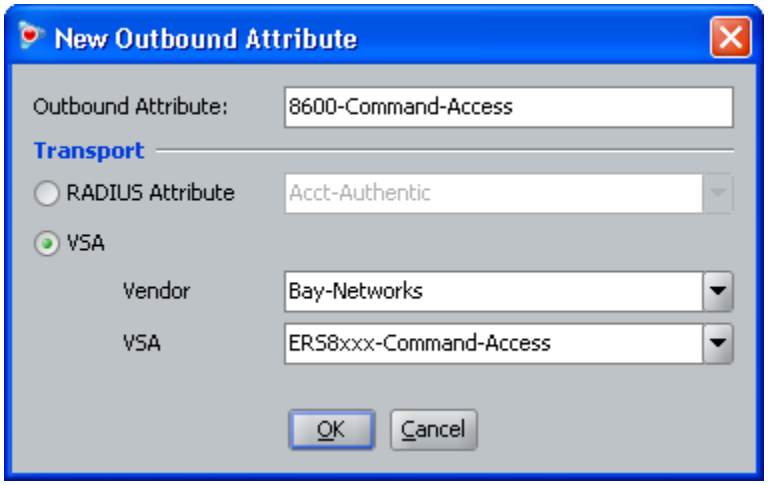


IDE Step 2 – Go to *Site Configuration -> Provisioning -> Outbound Attributes -> New*

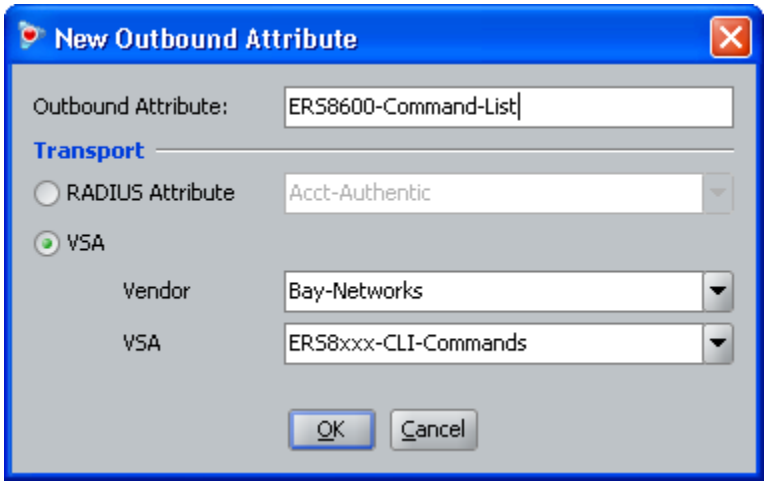


 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 3 – Via the *Outbound Attribute* window, type in a name for the attribute to be used to restrict CLI commands (i.e. 8600-Command-Access as used in this example), click the *VSA* radio button, select *Bay-Networks* via *Vendor* and *ERS8xxx-Command-Access* via *VSA*. Click on *OK* when done

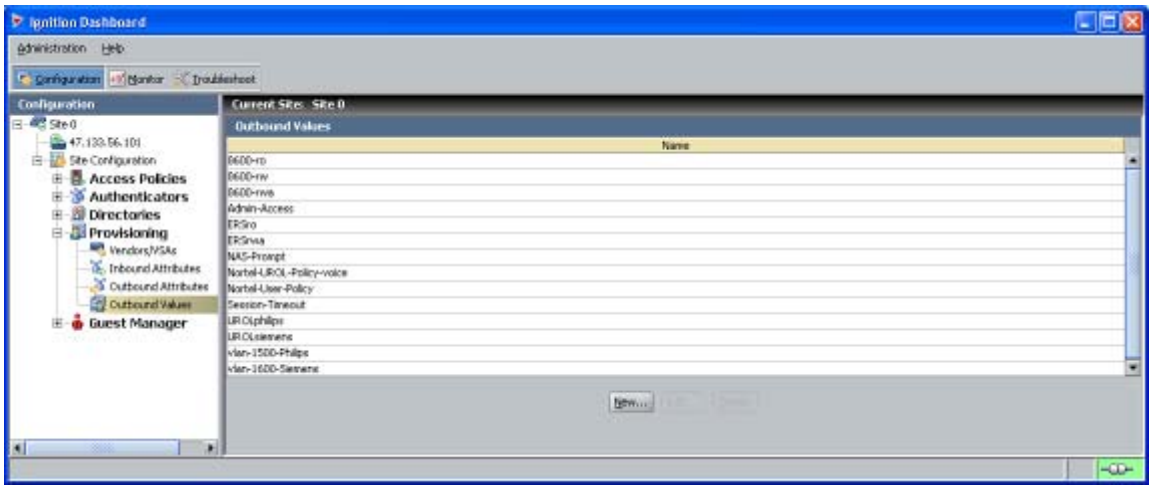


IDE Step 4 – Go to *Site Configuration -> Provisioning -> Outbound Attributes -> New* one more time. Via the *Outbound Attribute* window, type in a name for the attribute to be used to list the CLI commands (i.e. 8600-Command-List as used in this example), click the *VSA* radio button, select *Bay-Networks* via *Vendor* and *ERS8xxx-CLI-Commands* via *VSA*. Click on *OK* when done

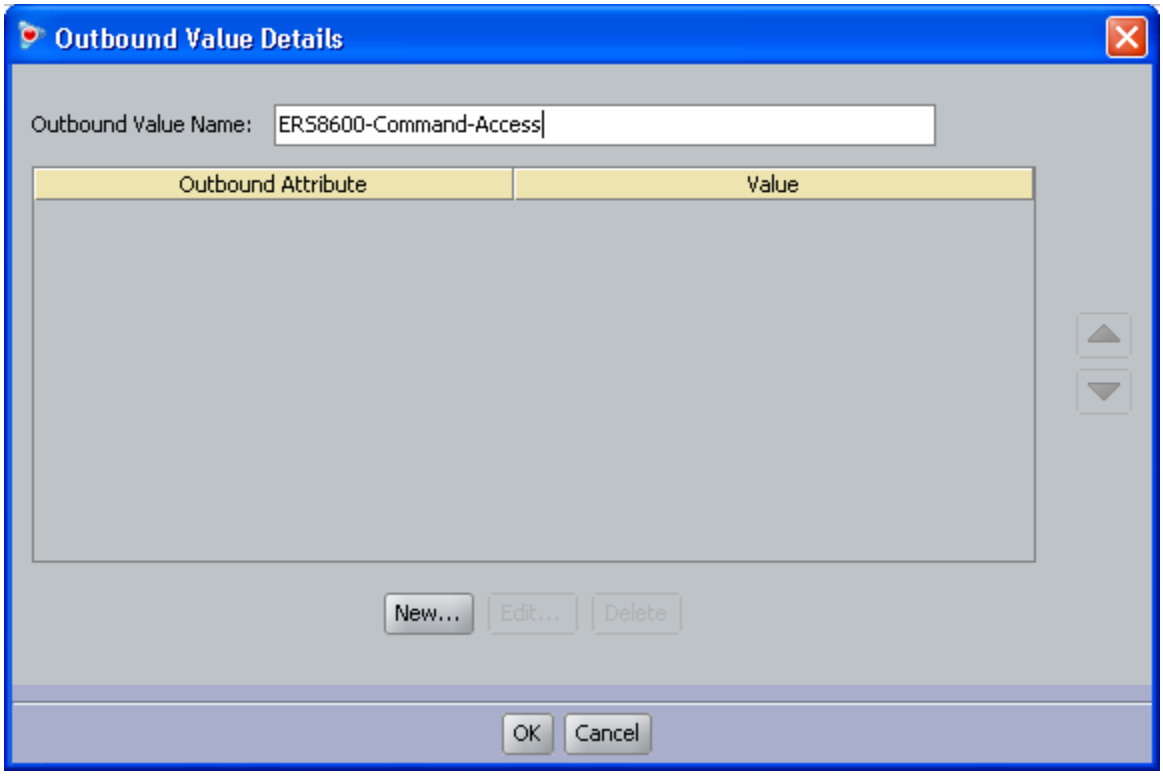


Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

IDE Step 5 – Go to *Site Configuration -> Provisioning -> Outbound Values -> New*

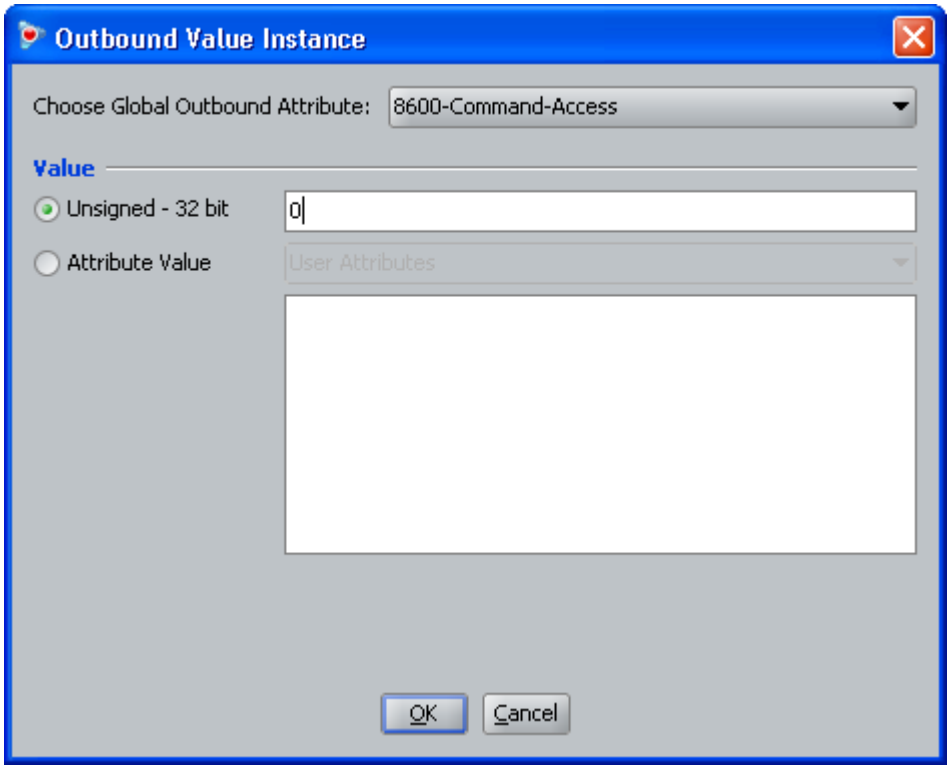


IDE Step 6 – Using the Outbound Attribute created in Step 3, we will add a value of 0 to restrict CLI command access. Start by entering a name via the *Outbound Value Name:* window (i.e. ERS8600-Command-Access as used in this example) and click on *New*



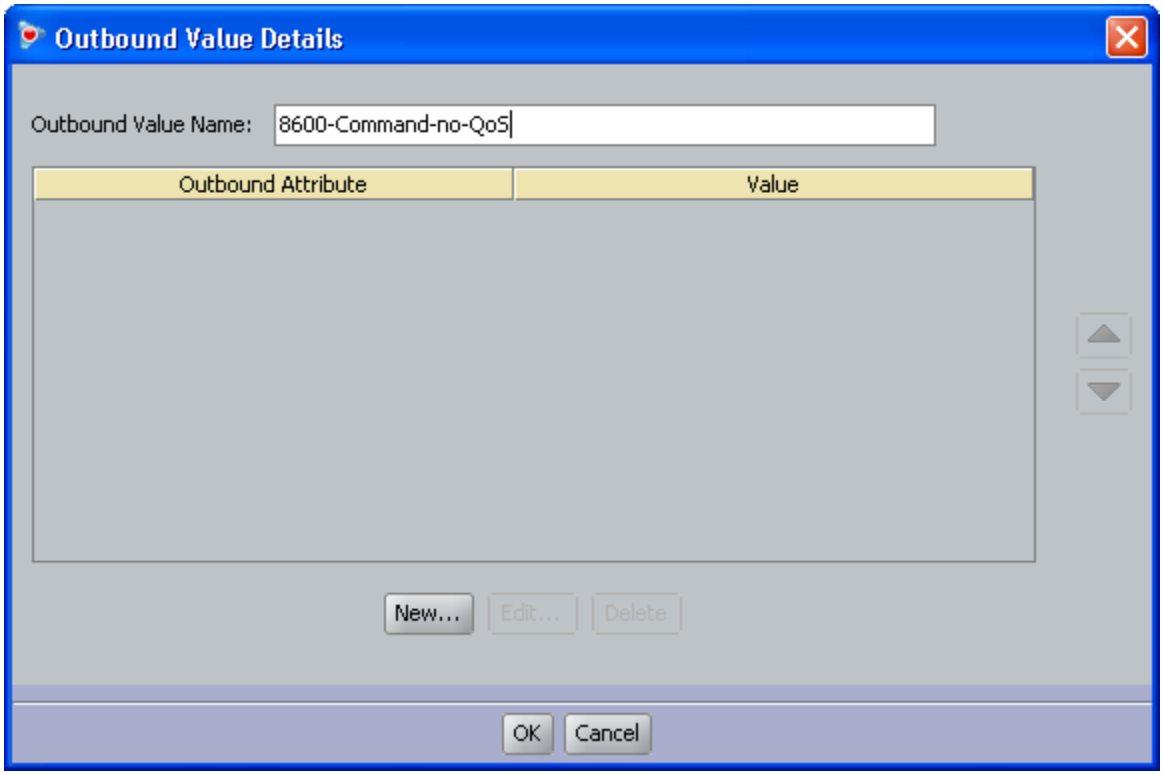
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 7 – Select the Outbound Attributes name created in Step 3 (i.e. ERS8600-Command-Access as used in this example) via the *Choose Global Outbound Attribute:* pull down menu. In the *Value Unsigned – 32 bit* window, enter 0 (i.e. value of 0 signifies CLI command restriction). Click on *OK* twice when done.



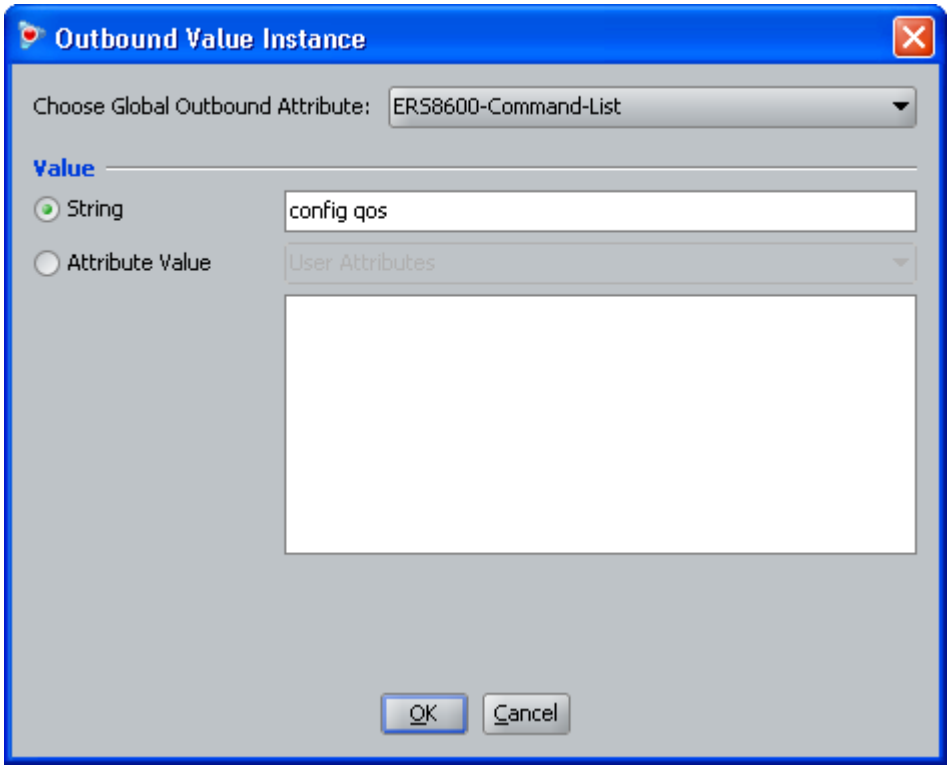
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 8 – Go to *Site Configuration -> Provisioning -> Outbound Values -> New* again to create the outbound attribute for deny access to the CLI command 'config qos'. Using the Outbound Attribute created in Step 4, we will add a string value of "config qos". Start by entering a name via the *Outbound Value Name:* window (i.e. 8600-Command-no-QoS as used in this example) and click on *New*



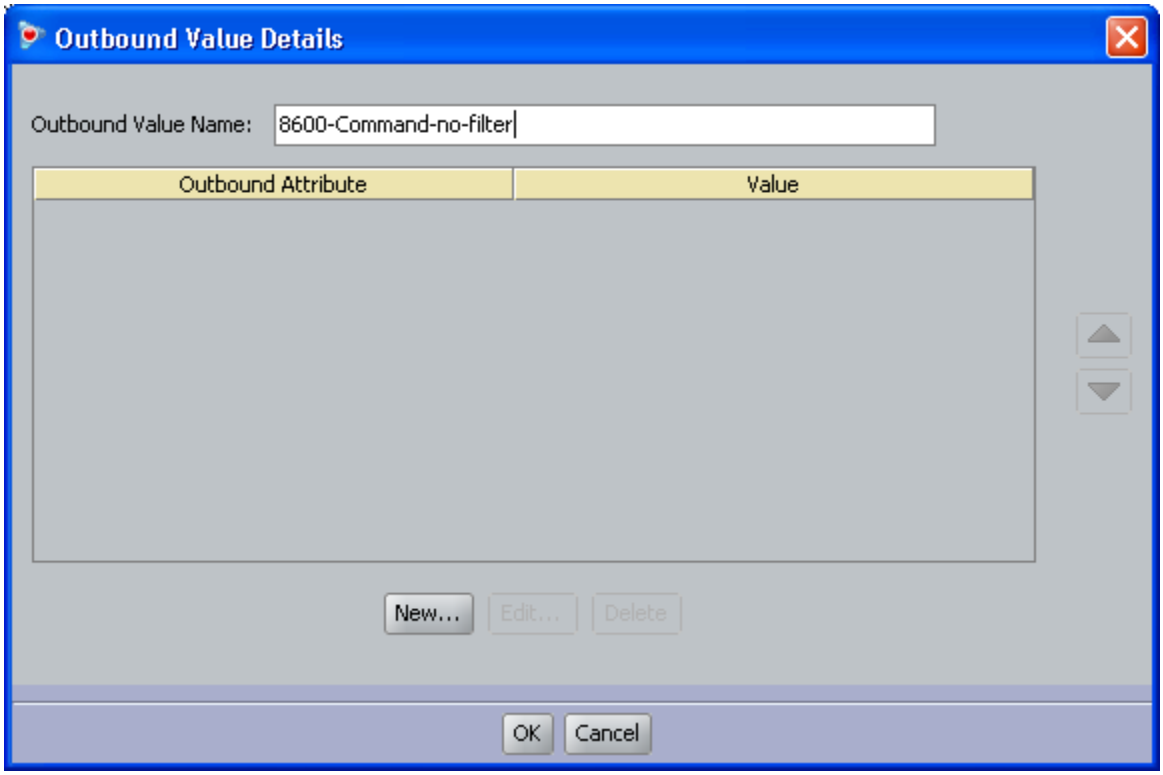
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 9 – Select the Outbound Attributes name created in Step 4 (i.e. ERS8600-Command-List as used in this example) via the *Choose Global Outbound Attribute:* pull down menu. In the *String* window, enter *config qos* (i.e. this is the CLI command we wish to restrict). Click on *OK* twice when done.



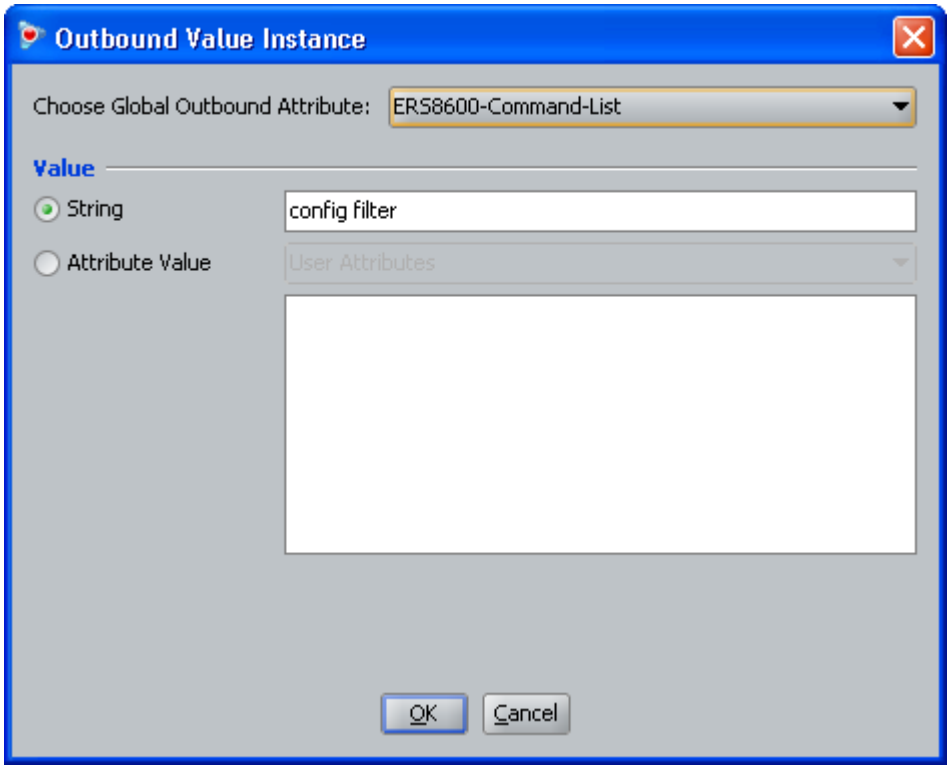
Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

IDE Step 10 – Go to *Site Configuration -> Provisioning -> Outbound Values -> New* again to create the outbound attribute for deny access to the CLI command 'config filter'. Using the Outbound Attribute created in Step 4, we will add a string value of "config filter". Start by entering a name via the *Outbound Value Name:* window (i.e. 8600-Command-no-filter as used in this example) and click on *New*



 Copyright © 2009 Nortel Networks. All Rights Reserved.

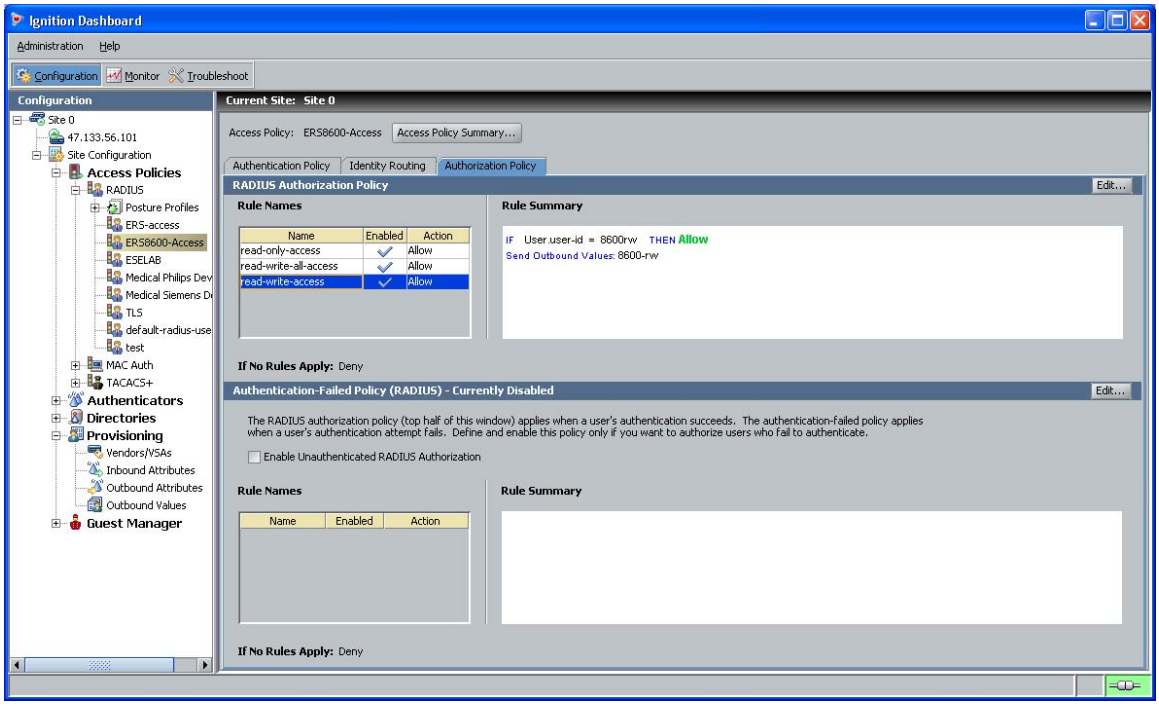
IDE Step 11 – Select the Outbound Attributes name created in Step 4 (i.e. ERS8600-Command-List as used in this example) via the *Choose Global Outbound Attribute:* pull down menu. In the *String* window, enter *config filter* (i.e. this is the CLI command we wish to restrict). Click on *OK* twice when done.



Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

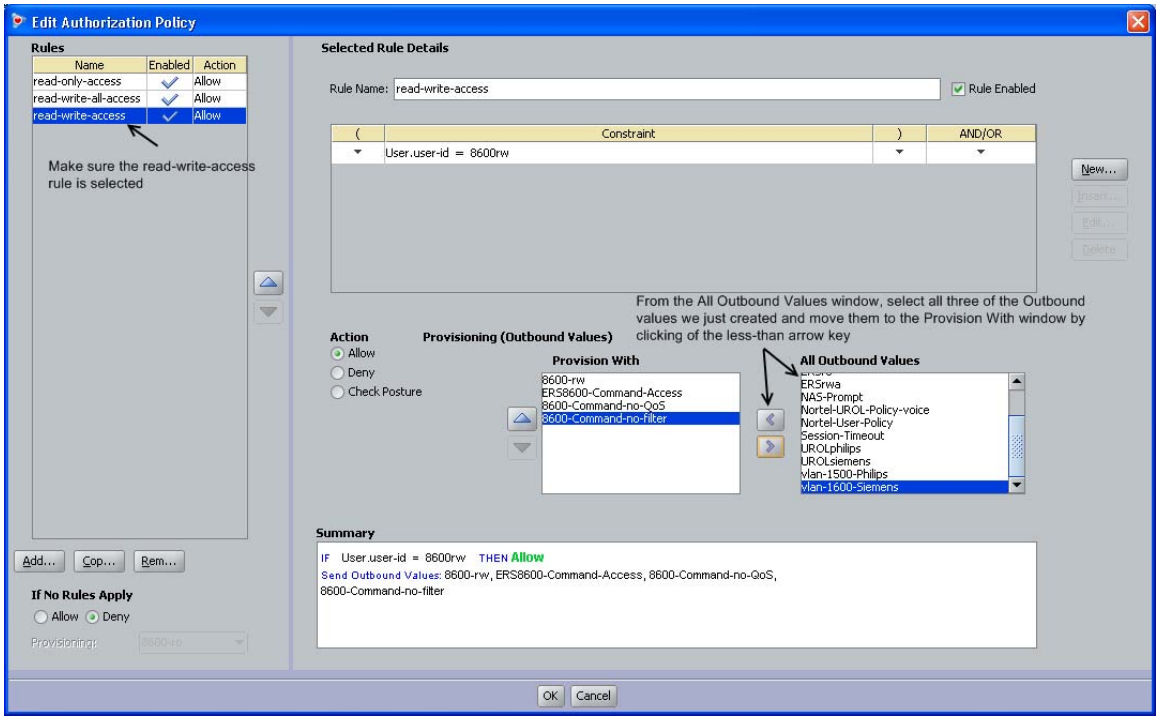
2.2.2.2 Modify the Authorization Policy for the ERS8600 read-write user

IDE Step 1 – Click on the policy created from the previous example, i.e. ERS8600-Access, click on the *Authorization Policy* tab, select the *read-write-access* via the *Rule Name* window, and click on Edit



 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 2 – Make sure the read-write-access rule is selected and move all three RADIUS attribute values we just created from the previous step from the *All Outbound Values* window to the *Provision With* window



 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 3 – When completed, you can view the complete policy by clicking on the *Access Policy Summary* button

 Copyright © 2009 Nortel Networks. All Rights Reserved.

2.2.3 Verification

Connect to ERS8600 by using telnet with the read-write user account.

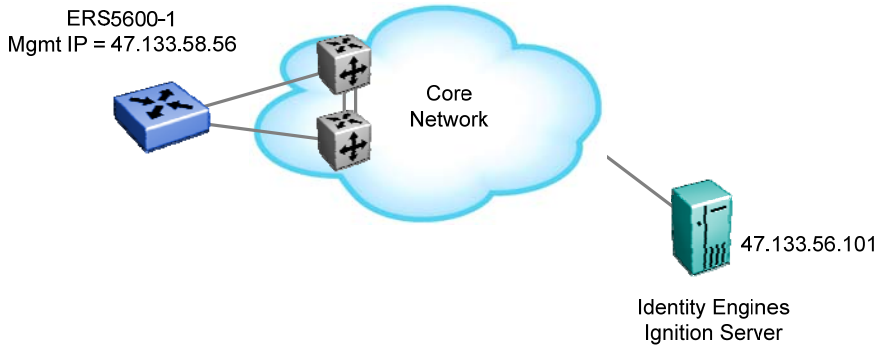
ERS8600-1 – Verify operation by typing in some commands

```
ERS-8606:5# config qos

Permission denied.

ERS-8606:5# config filter

Permission denied.
```

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.

External Distribution

3. ERS5600 Switch Configuration Example



For this configuration example, we will enable RADIUS user authentication on ERS500-1 using the switch management port. We will configure the Identity Engines RADIUS server with the following two users:

- User name with read-only access: 5600ro
- User name with read-write access: 5600rw

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

3.1 ERS5600 Configuration

3.1.1 Enable RADIUS

Up to two RADIUS servers are supported on the ERS5600, 5500, 4500, or 2500 series switches. For this configuration example we will simply configure one RADIUS server.

ERS5698-1 Step 1 – Add RADIUS server, enable RADIUS, and enable RADIUS accounting
5698TFD-1-PWR(config)#***radius-server host 47.133.56.101 key Nortel***
5698TFD-1-PWR(config)#***radius accounting enable***
5698TFD-1-PWR(config)#***cli password telnet radius***
If the switch is used in a stack, enter the following:
5698TFD-1-PWR(config)#***cli password stack telnet radius***
ERS5698-1 Step 1 – Optional, enabling password fallback
5698TFD-1-PWR(config)#***radius-server password fallback***

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

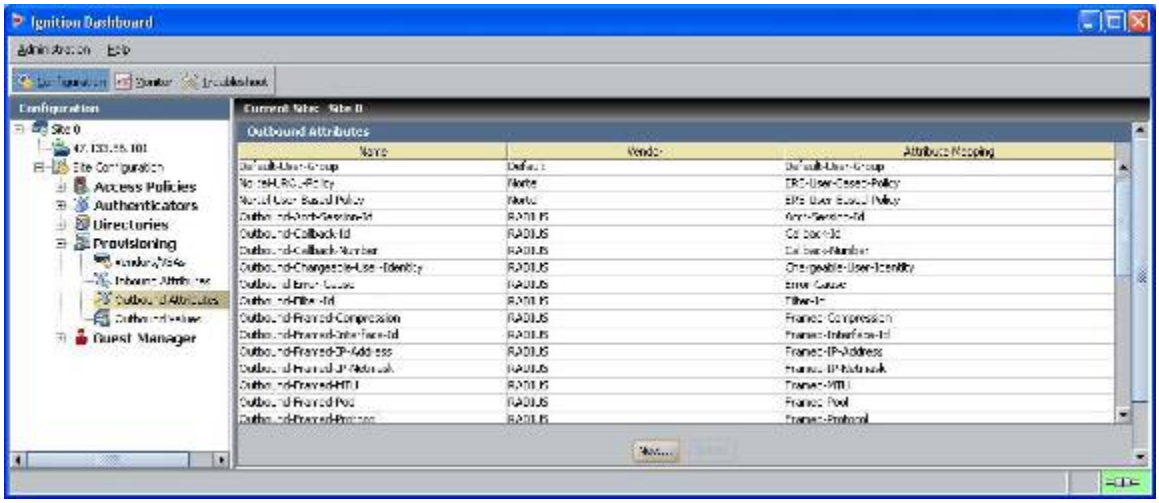
3.2 IDE Setup

3.2.1 Configure an Outbound Attribute on Ignition Server for Service-Type

The following chart displays the outbound attribute values required by the ERS5600, ERS5500, ERS4500, or ERS2500 for each access level using RADIUS attribute type 6 (Service-Type).

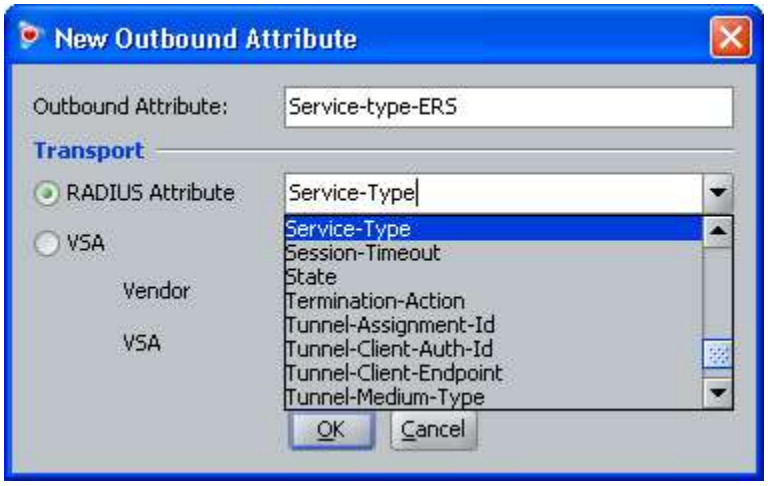
Registry Value	Description	ERS Access Level
6	Administrative	Read-Write-All-Access
7	NAS Prompt	Read-Only-Access

IDE Step 1 – Go to *Site Configuration -> Provisioning -> Outbound Attributes -> New*

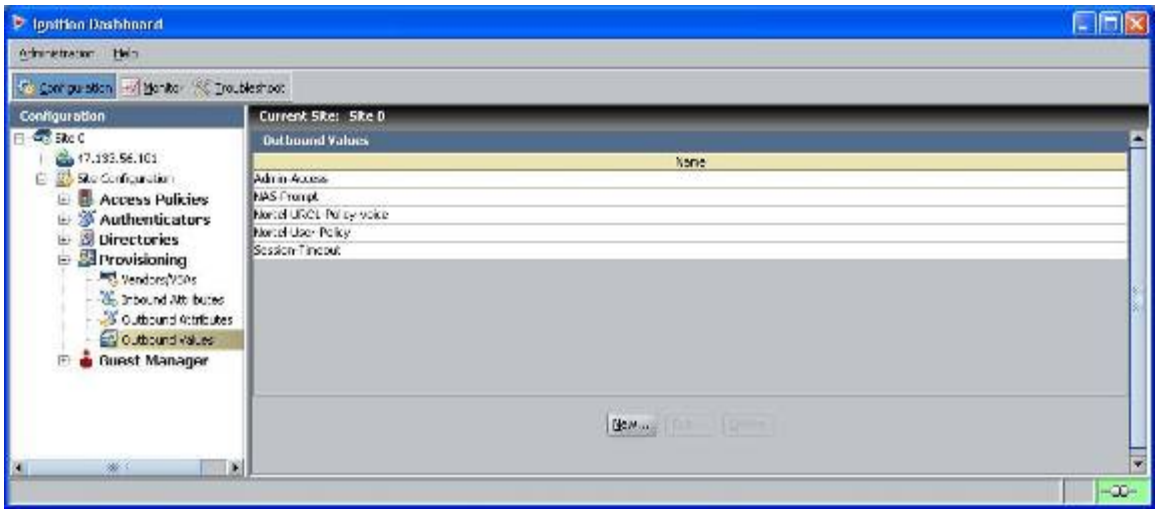


 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 2 – Via the *Outbound Attribute* window, type in a name for the attribute to be used for access priority (i.e. Service-type-ERS as used in this example), click the *RADIUS Attribute* radio button and select *Service-Type*. Click on *OK* when done

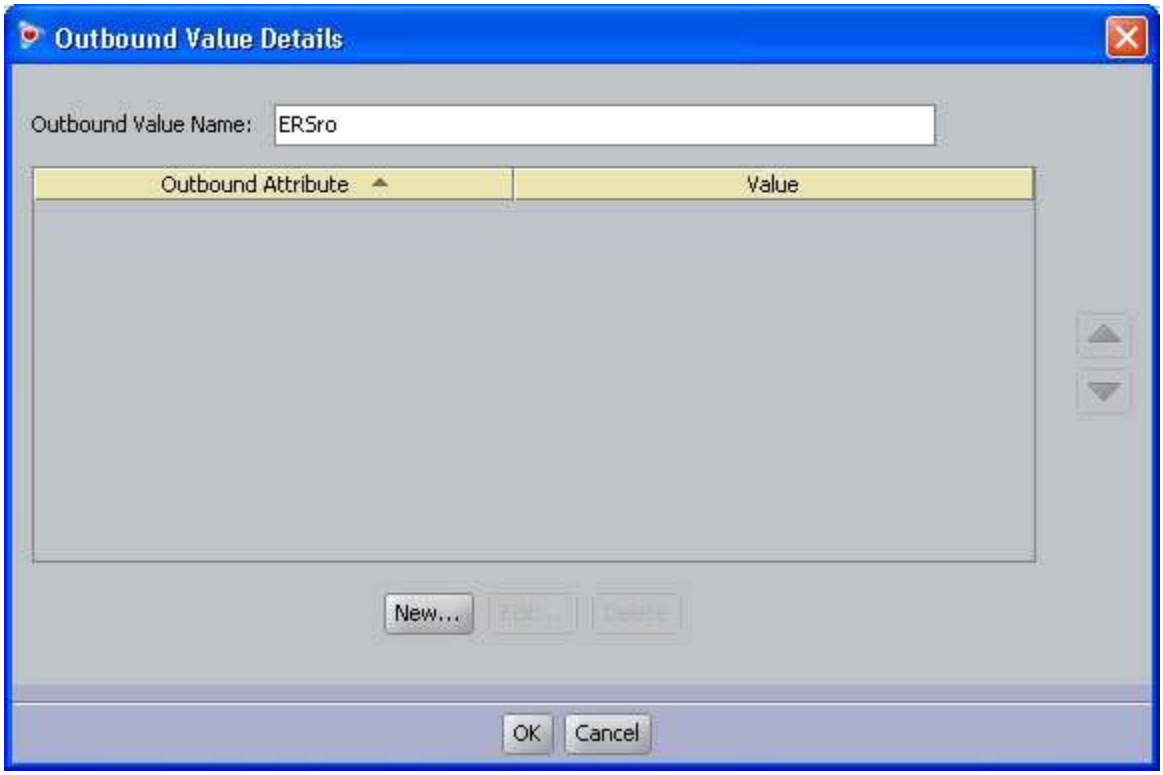


IDE Step 4 – Go to *Site Configuration -> Provisioning -> Outbound Values -> New*



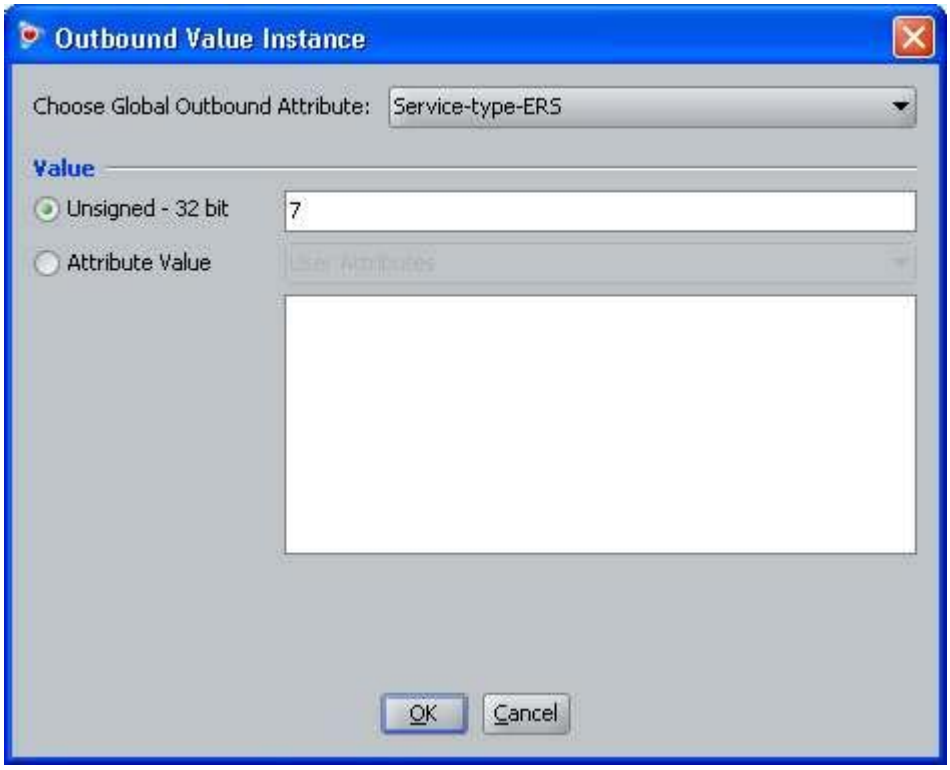
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 5 – Using the Outbound Attribute created in Step 2, we will first add a value of 7 (NAS Prompt) for read-only-access. Start by entering a name via the *Outbound Value Name:* window (i.e. ERSro as used in this example) and click on *New*



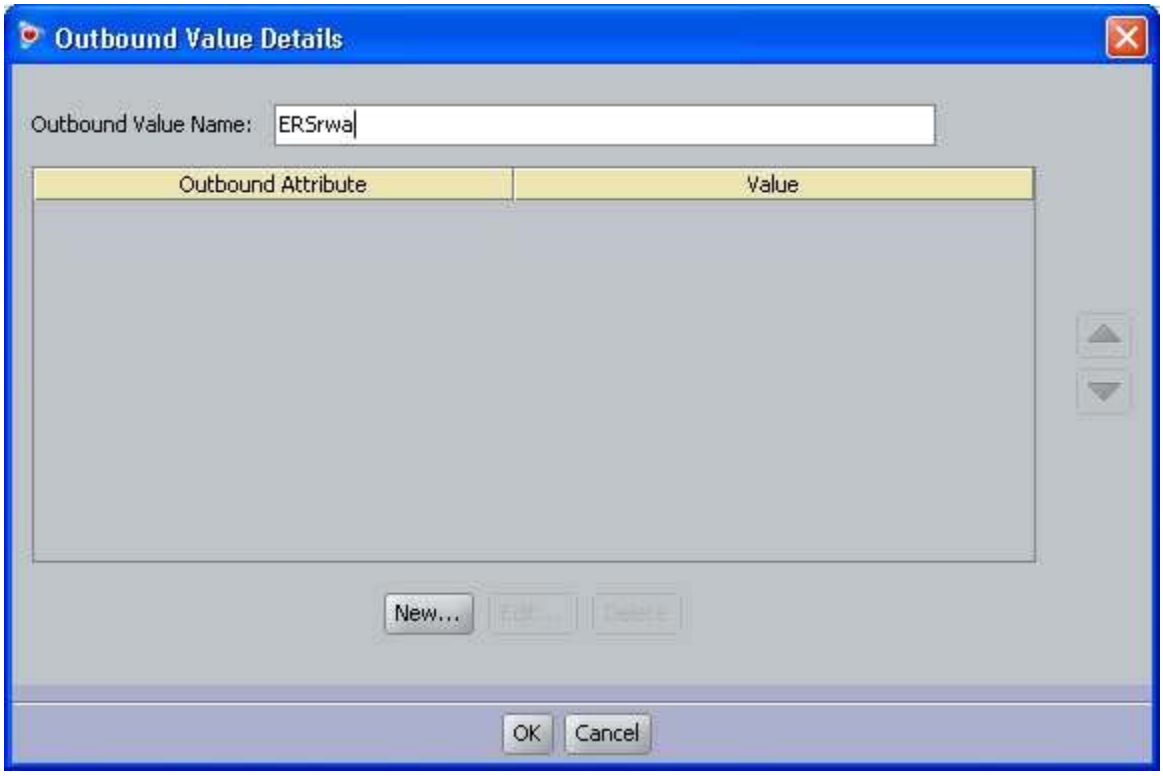
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 6 – Select the Outbound Attributes name created in Step 3 (i.e. Service-type-ERS as used in this example) via the *Choose Global Outbound Attribute:* pull down menu. In the *Value Unsigned – 32 bit* window, enter 7 (i.e. value of 7 signifies NAS Prompt for read-only-access). Click on *OK* twice when done.



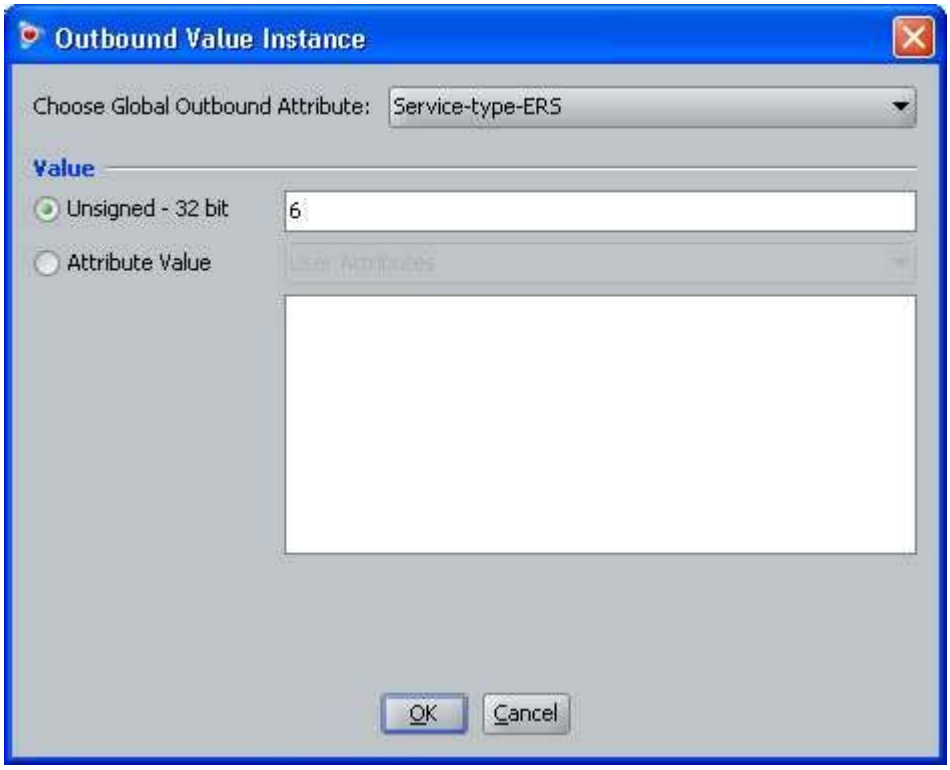
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 7 – Go to *Site Configuration -> Provisioning -> Outbound Values -> New* again to create the outbound attribute for read-write-access. Using the Outbound Attribute created in Step 2, we will add a value of 6 for read-write-access. Start by entering a name via the *Outbound Value Name:* window (i.e. ERSrwa as used in this example) and click on *New*



Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

IDE Step 8 –Select the Outbound Attributes name created in Step 2 (i.e. Service-type-ERS as used in this example) via the *Choose Global Outbound Attribute:* pull down menu. In the *Value Unsigned – 32 bit* window, enter 6 (i.e. value of 6 signifies Administrative for read-write-access). Click on *OK* twice when done.



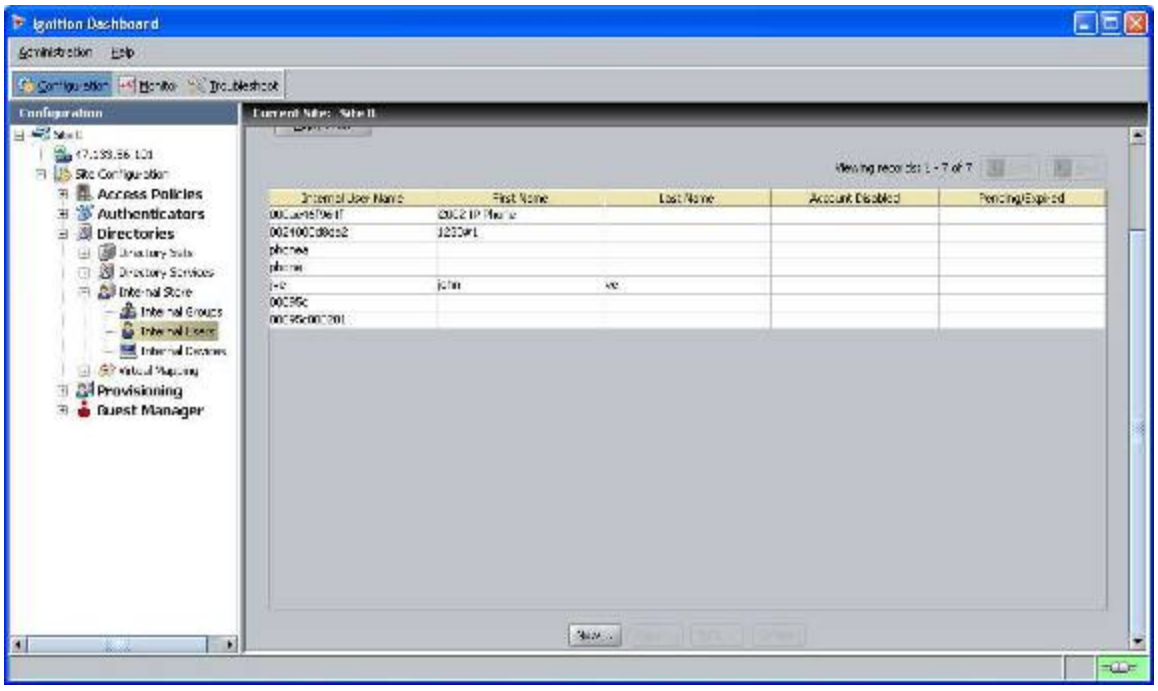
 Copyright © 2009 Nortel Networks. All Rights Reserved.

3.2.2 Add Users

For this configuration example, we will add the following users

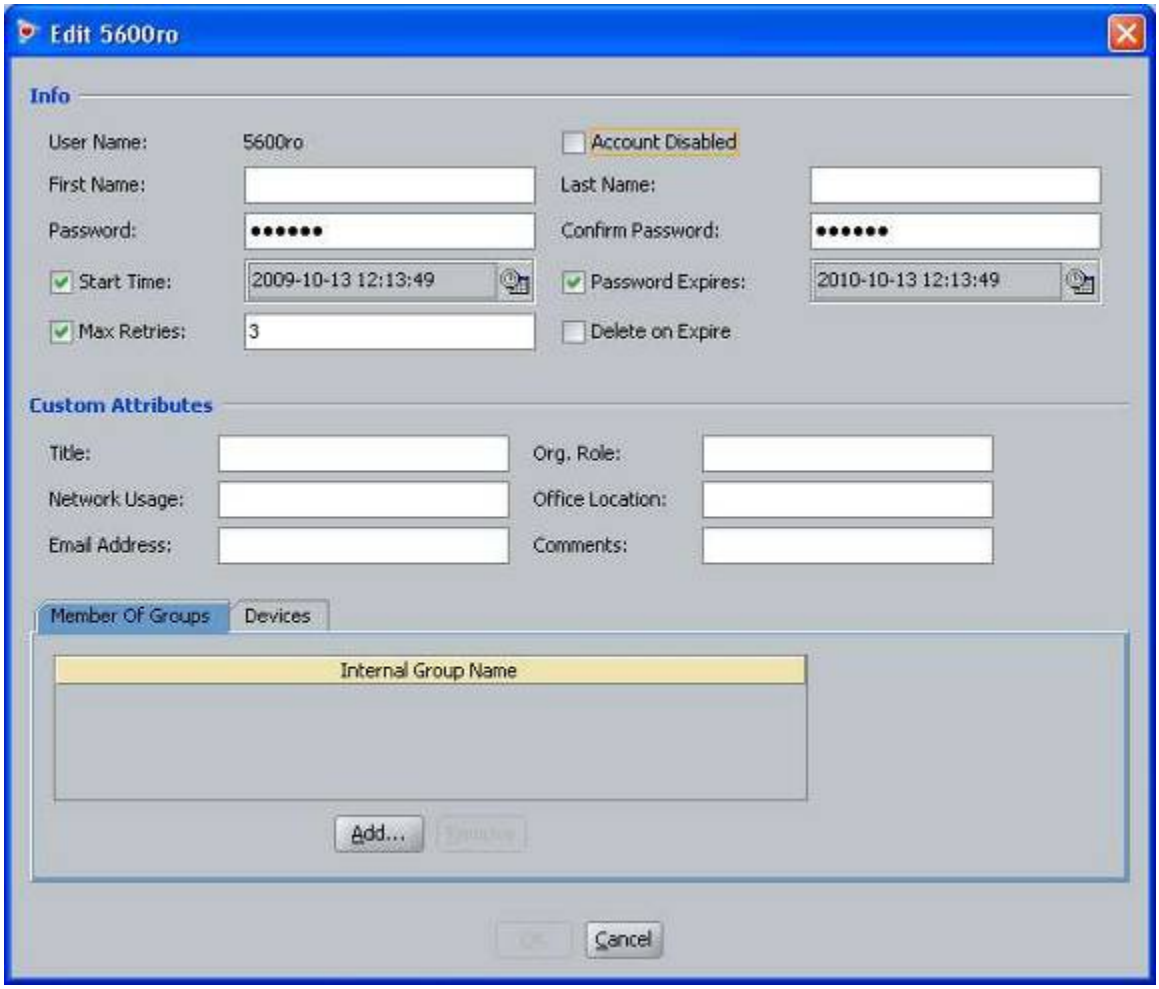
User Name	Access Level
5600ro	Read-Only-Access
5600rwa	Read-Write-All-Access

IDE Step 1 – Start by going to *Site Configuration -> Directories -> Internal Store -> Internal Users* and click on *New*



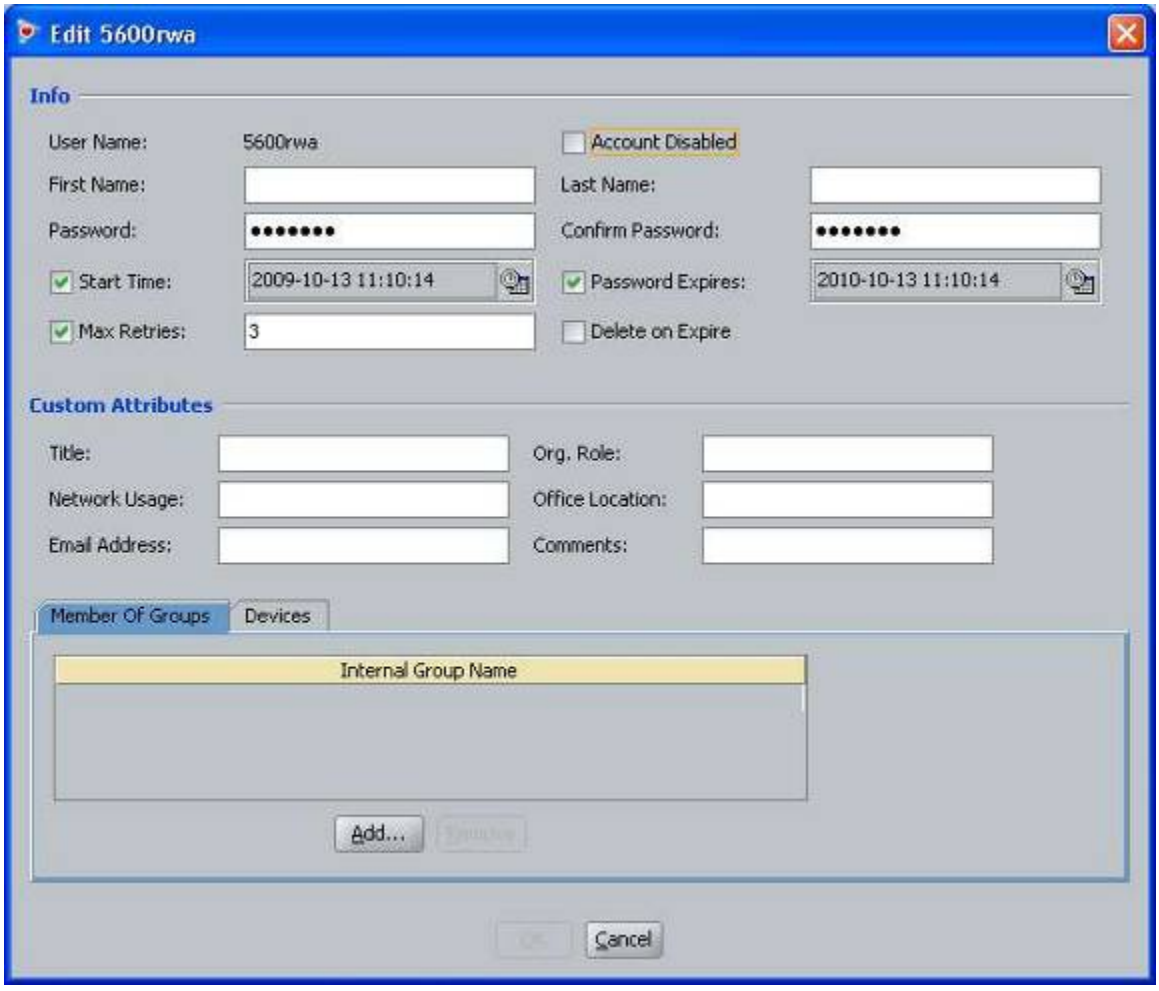
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 2 – Enter the user name for read-only-access via *User Name:* (i.e. 5600ro as used in this example) and enter the password for this user via *Password* and *Confirm Password*. Click on *OK* when done. If you wish, you can also change the expiry date via *Password Expires* if you do not wish to use the default setting of one year



 Copyright © 2009 Nortel Networks. All Rights Reserved.

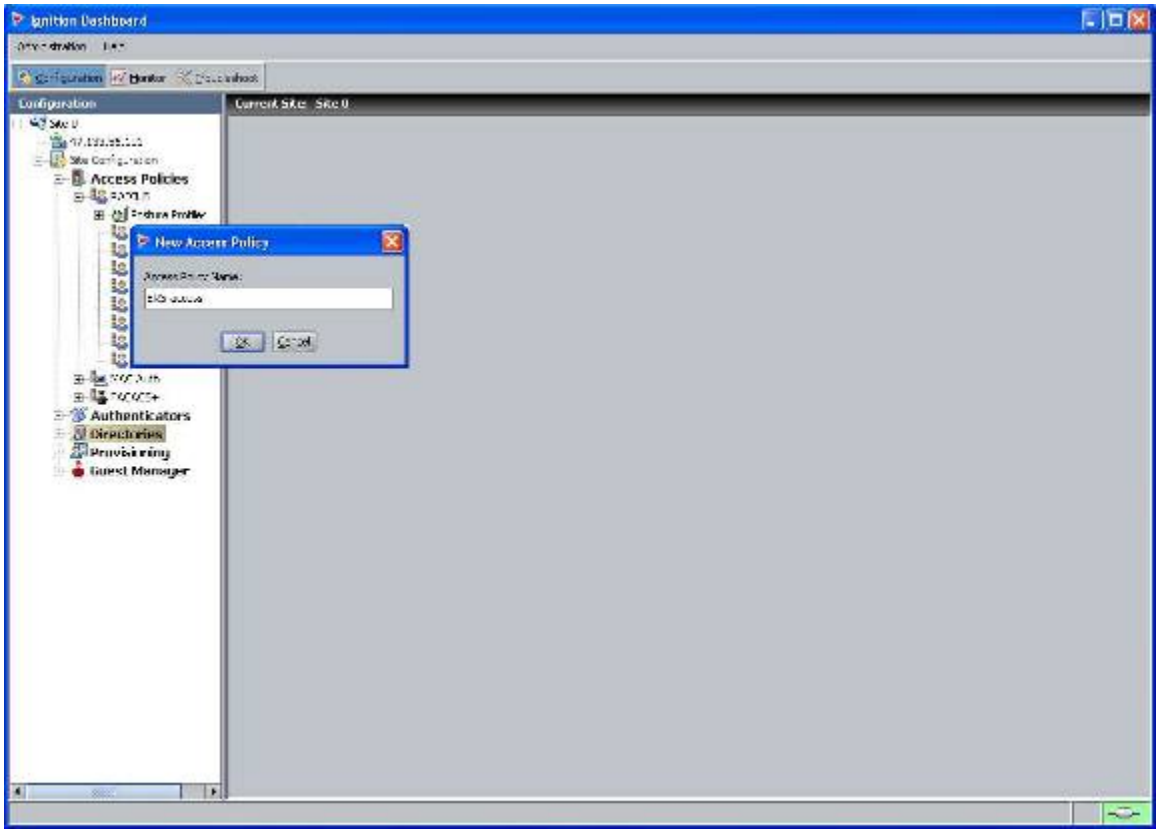
IDE Step 3 – Repeat step 2 again by clicking on New to add the read-write-access user. Enter the user name for read-write-access via *User Name:* (i.e. 5600rw as used in this example) and enter the password for this user via *Password* and *Confirm Password*. Click on *OK* when done. If you wish, you can also change the expiry date via *Password Expires* if you do not wish to use the default setting of one year



 Copyright © 2009 Nortel Networks. All Rights Reserved.

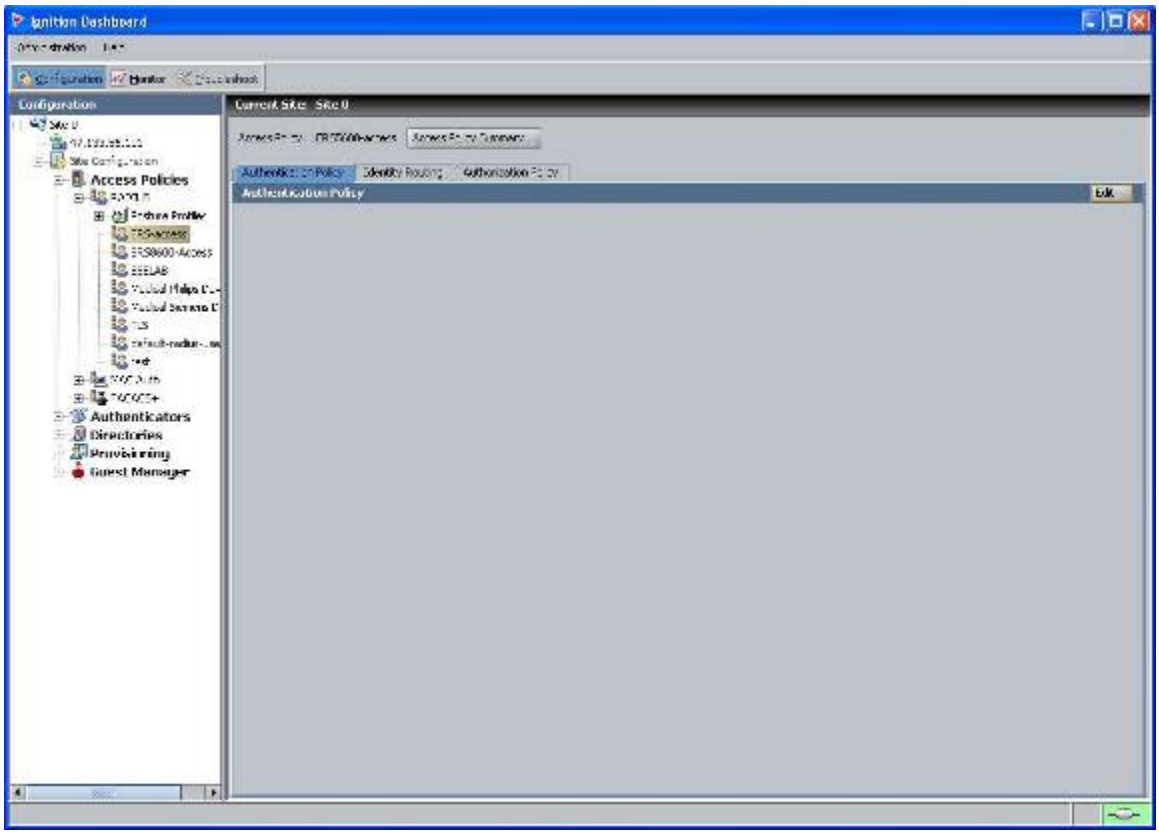
3.2.3 Add Access Policy

IDE Step 1 – Go to *Site Configuration -> Access Policies -> RADIUS.* Right-click R*ADIUS* and select *New Access Policy*. Enter a policy name, i.e. ERS-access as used in this example and click on *OK* when done



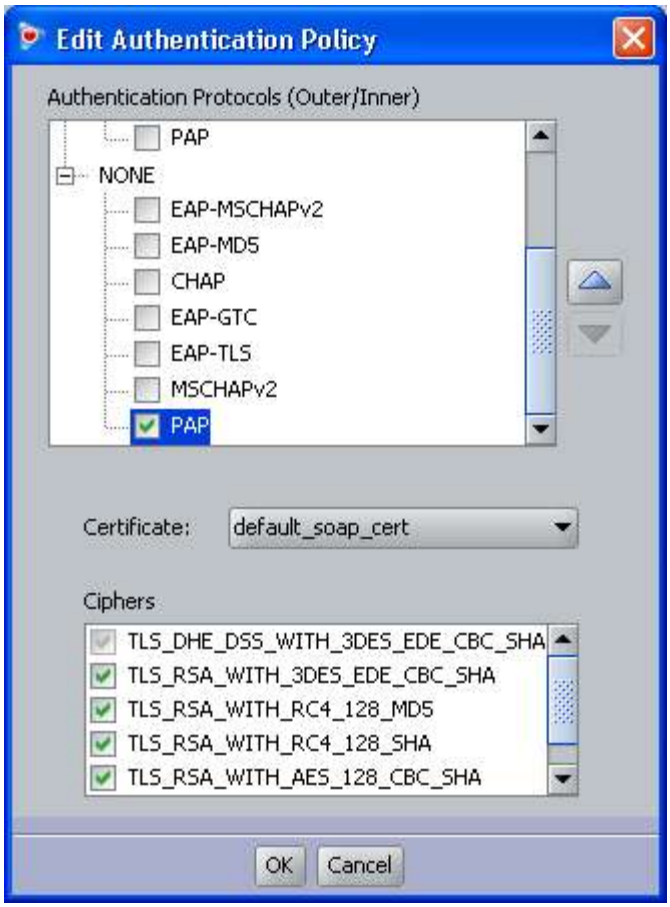
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 2 – Click on the policy we just created, i.e. ERS-access, and click on *Edit* via the *Authentication Policy* tab



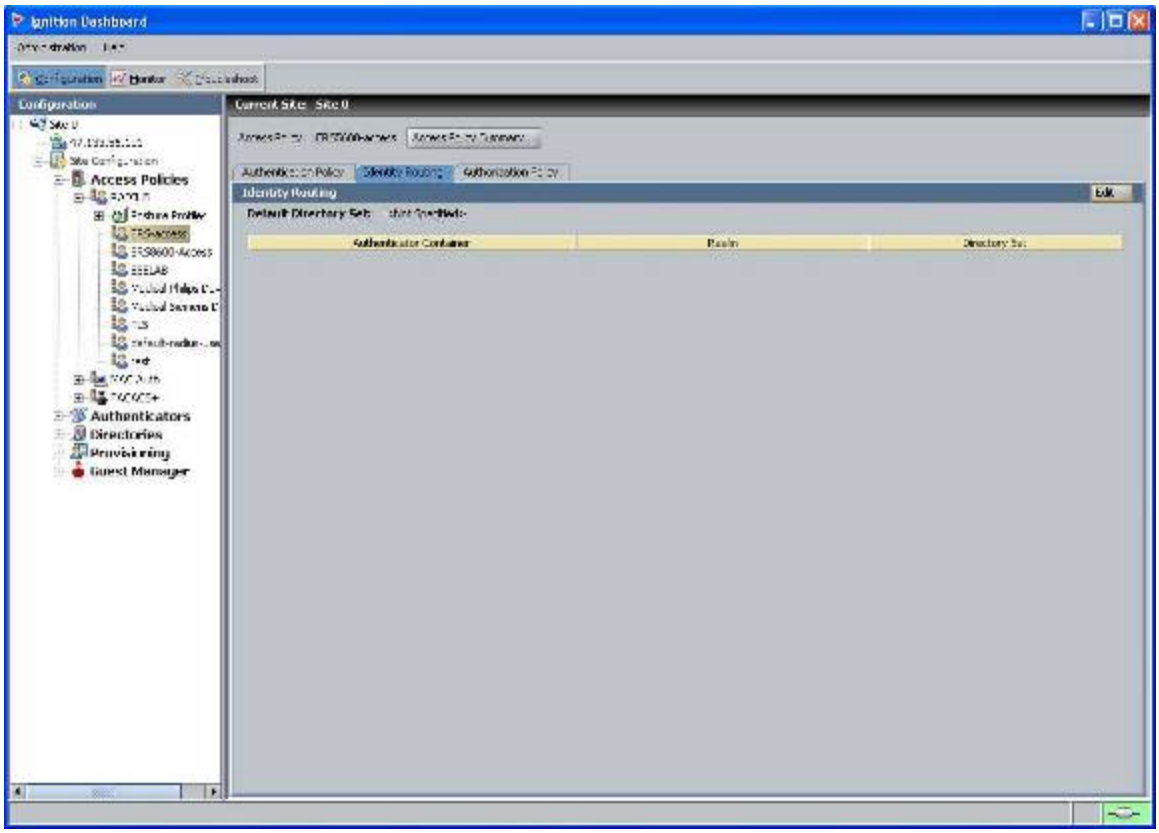
Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

IDE Step 3 – Under *Edit Authentication Policy* window, select *NONE -> PAP*



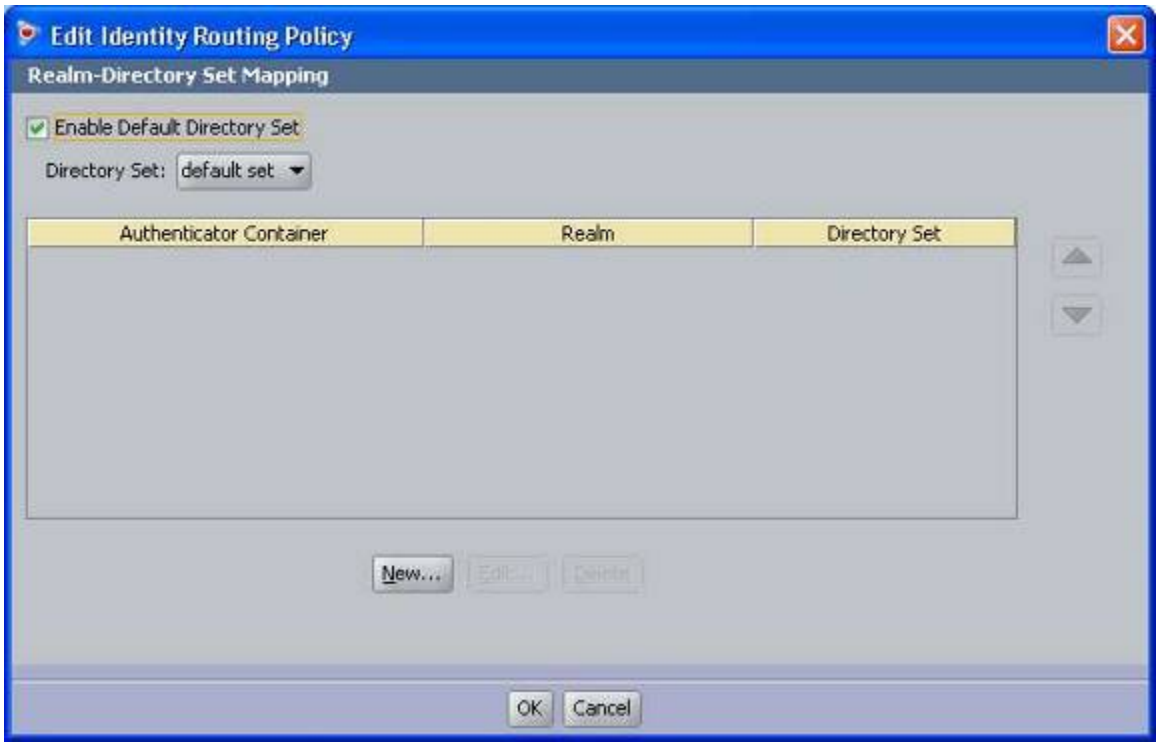
Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

IDE Step 4 – Go to the *Identity Routing tab* and click on *Edit*



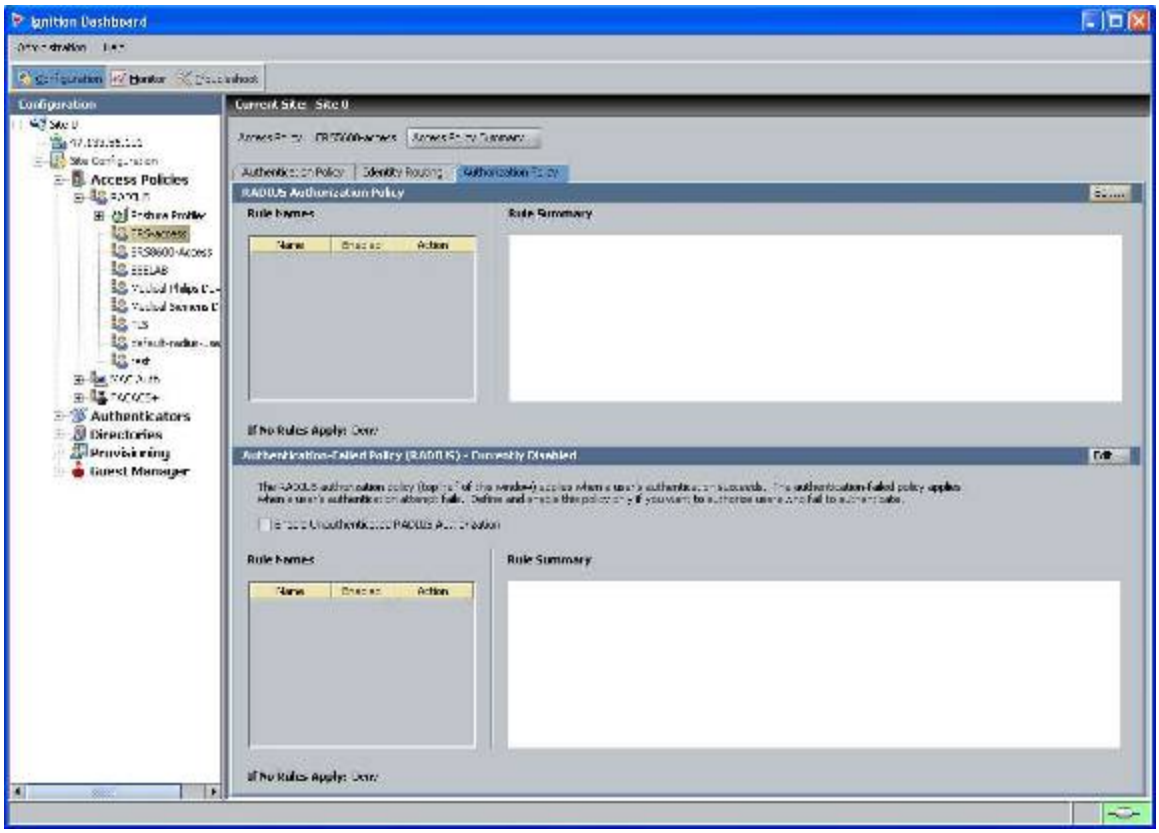
Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

IDE Step 5 – Check off the *Enable Default Directory Set* and click on *OK* when done.



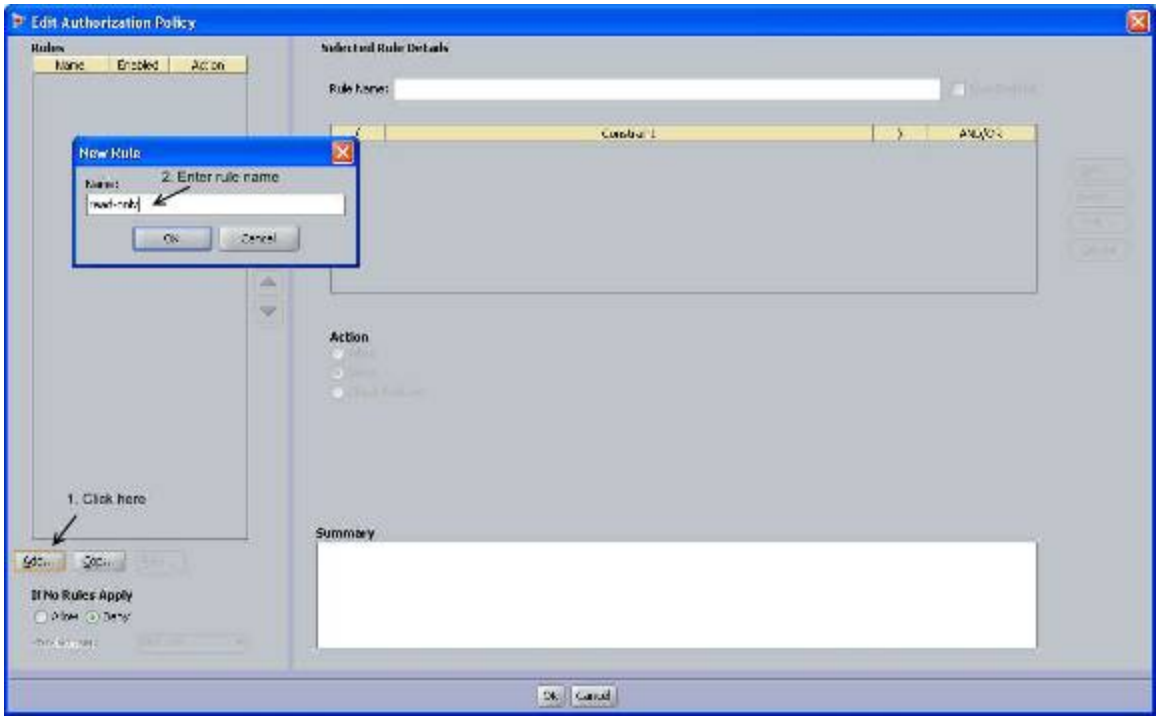
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 6 – Go to the *Authorization Policy* tab and click on *Edit*



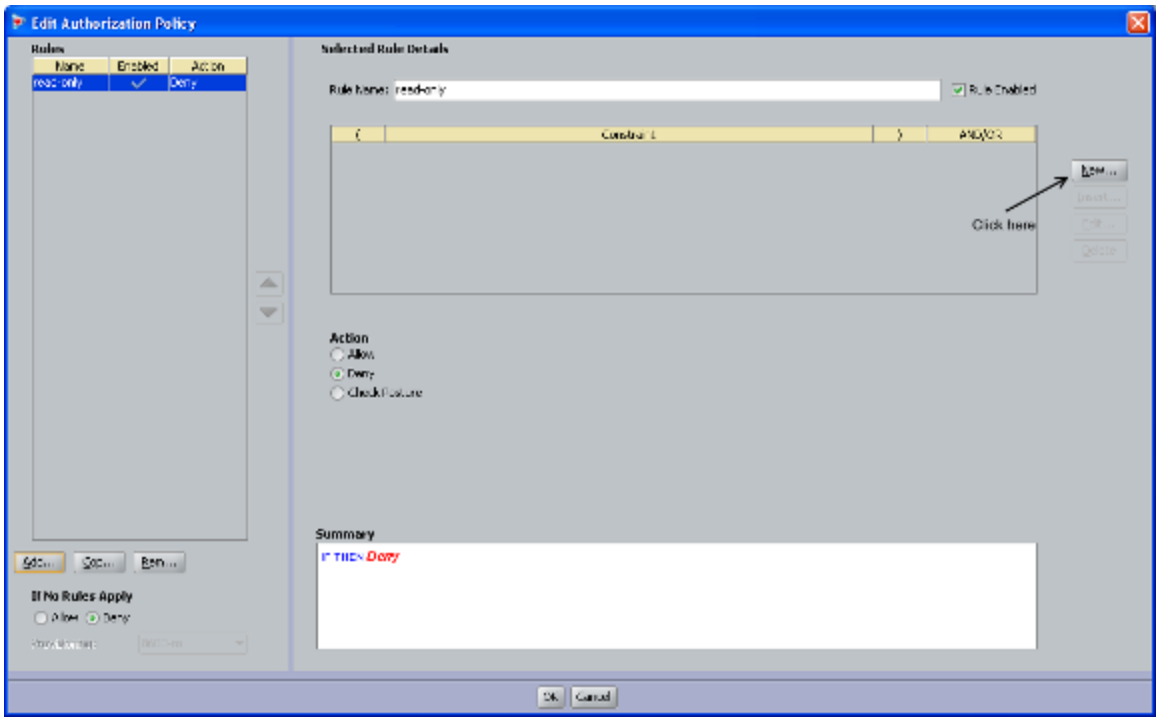
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 7 – Once the *Edit Authorization Policy* window pops up, click on *Add.* First, we will add a rule for read-only. When the *New Rule* window pops up, we will name the rule *read-only* as shown below



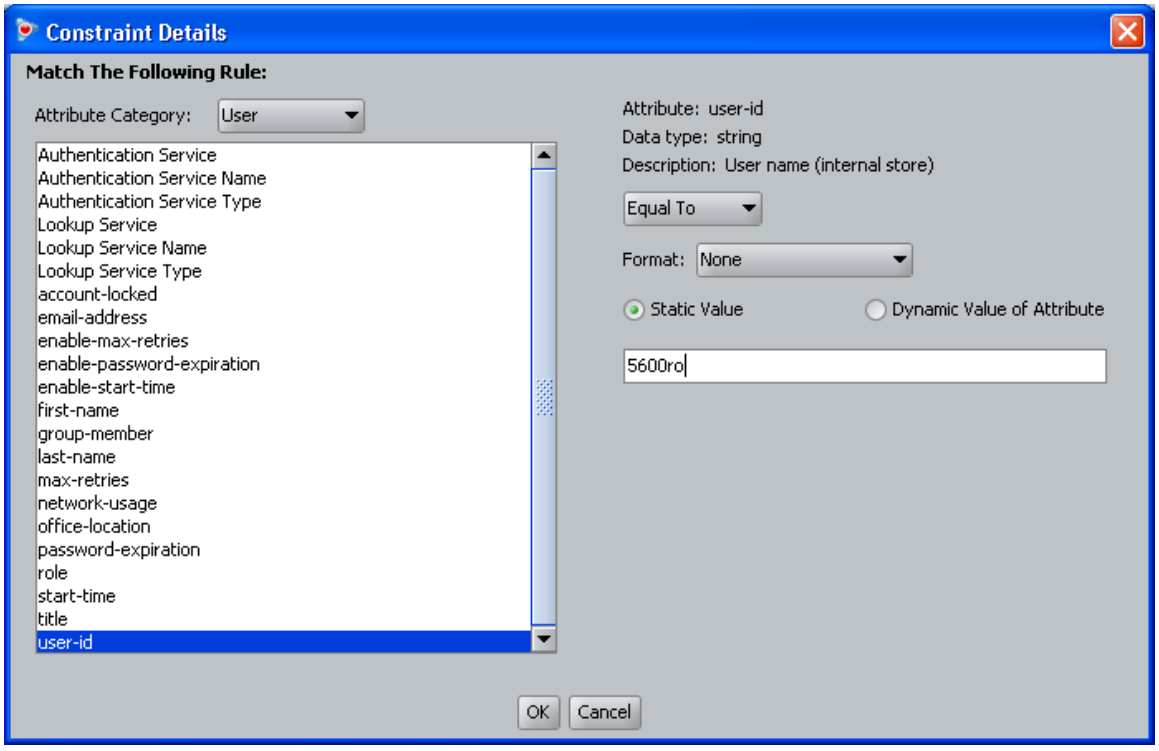
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 8 – Click on *New* to add a new constraint



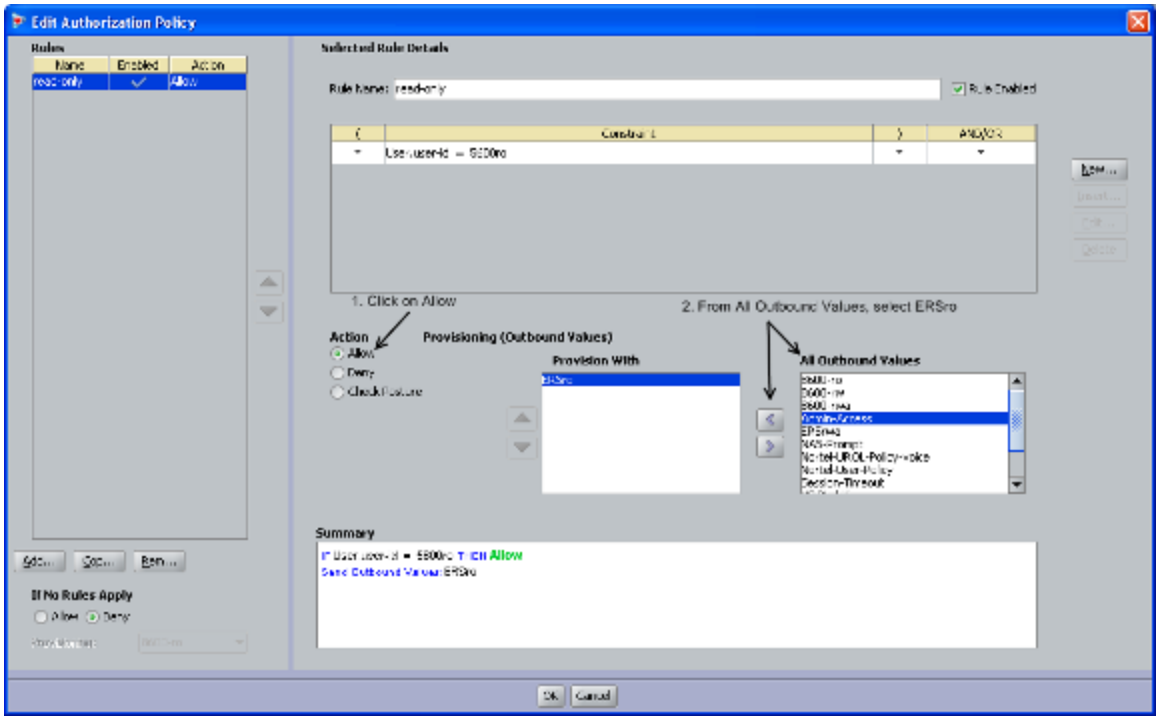
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 8 – For this example, we are simply going to look for the read-only-user user-id. From *Attribute Category*, select *User* and scroll down and select *user-id*. Select *Equal To* with *Format* of *None* and enter the read-only-access user id, i.e. 5600ro as used in this example, in the *Static Value* window as shown below. Click on *OK* when done



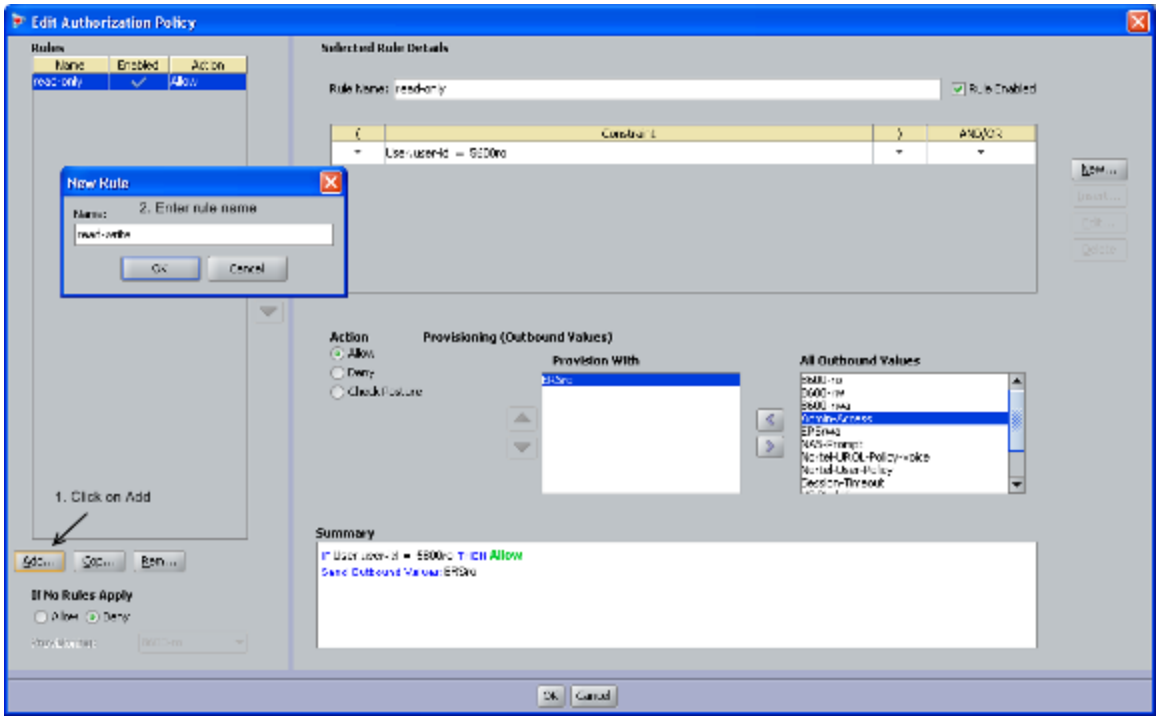
Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

IDE Step 9 – Via *Action*, select *Allow*. From the *All Outbound Values* window, select the output attribute we created above named *ERSro* and click on the less-than arrow key to move the attribute to the *Provision With* window



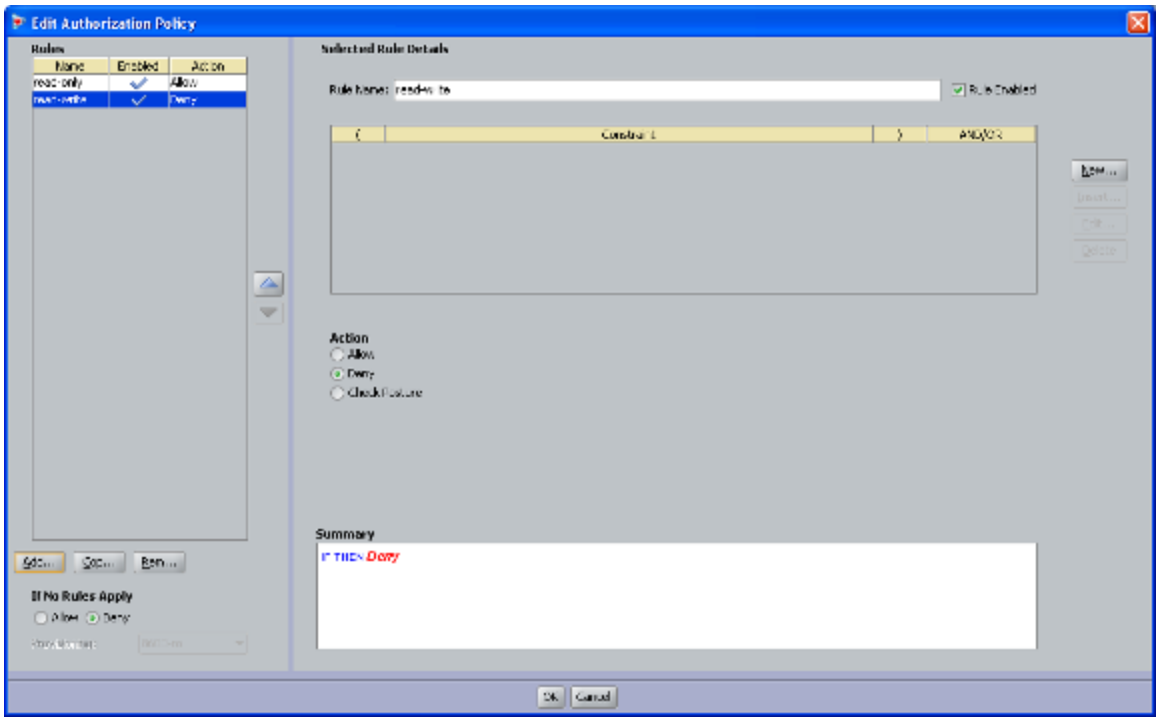
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 10 – Next, we will add a rule for read-write-access. Start by clicking on *Add* and when the *New Rule* window pops up, add an appropriate name for this rule, i.e. *read-write* as used in this example



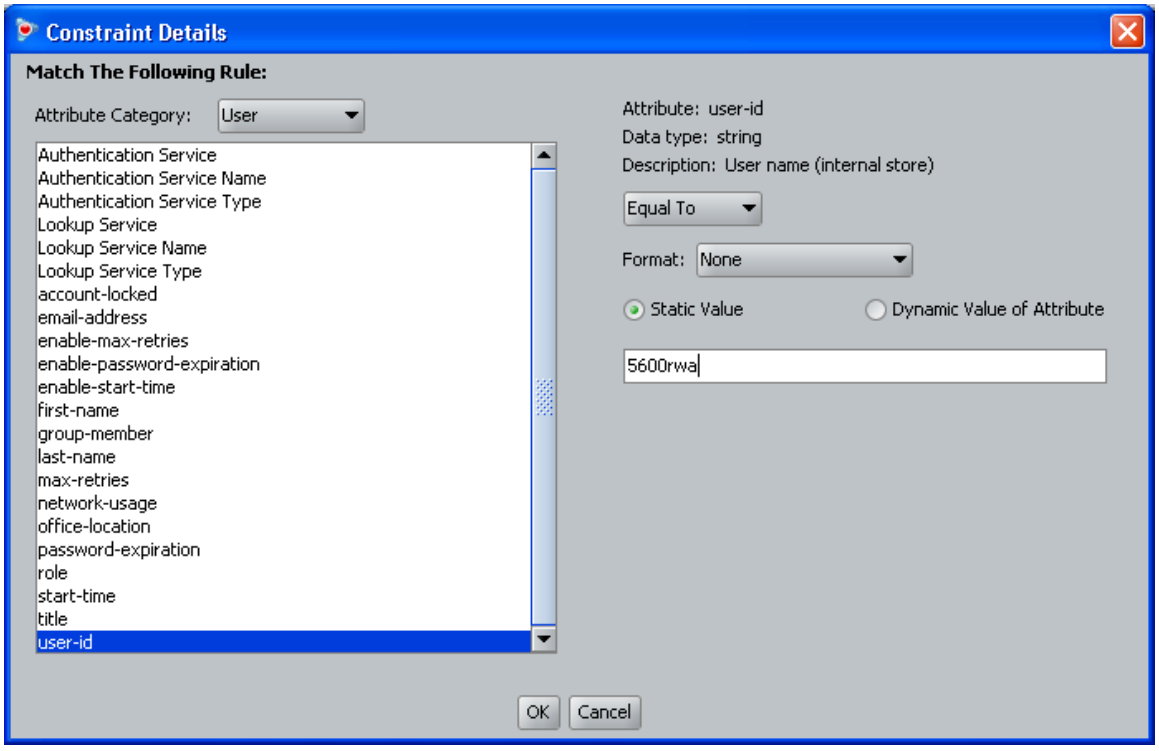
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 11 – Click on *New* to add a new constraint



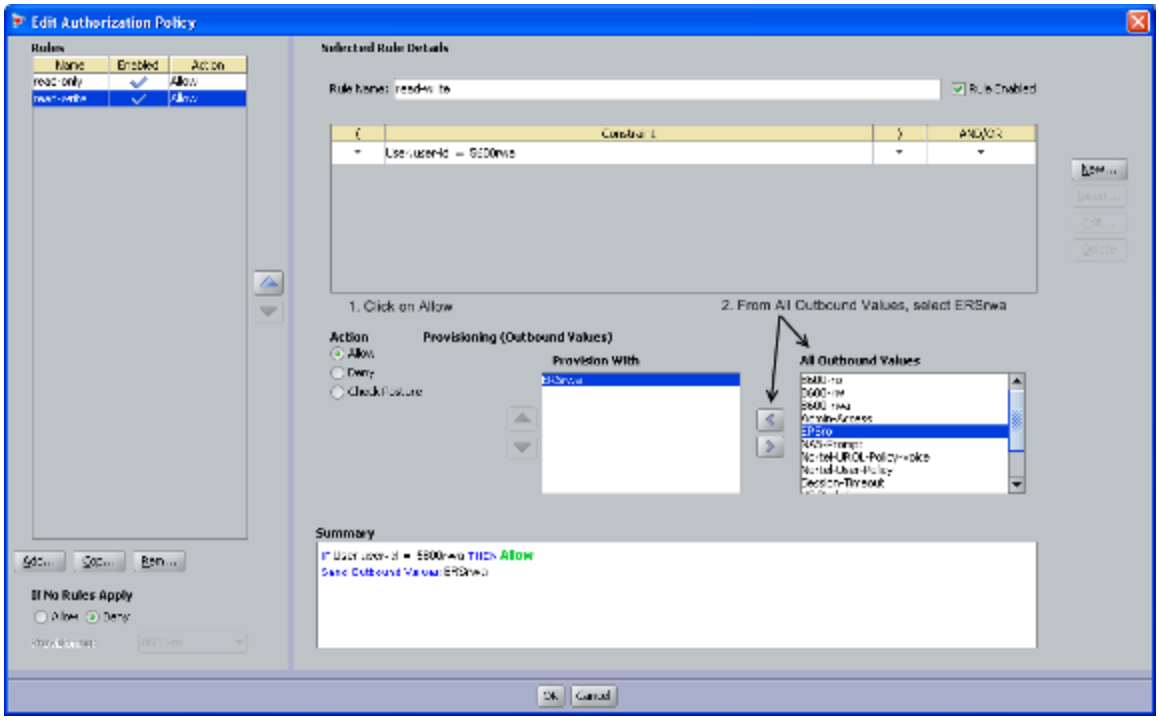
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 12 – For this example, we are simply going to look for the read-write user-id. From *Attribute Category*, select *User* and scroll down and select *user-id*. Select *Equal To* with *Format* of *None* and enter the read-write user id, i.e. 5600rwa as used in this example, in the *Static Value* window as shown below. Click on *OK* when done



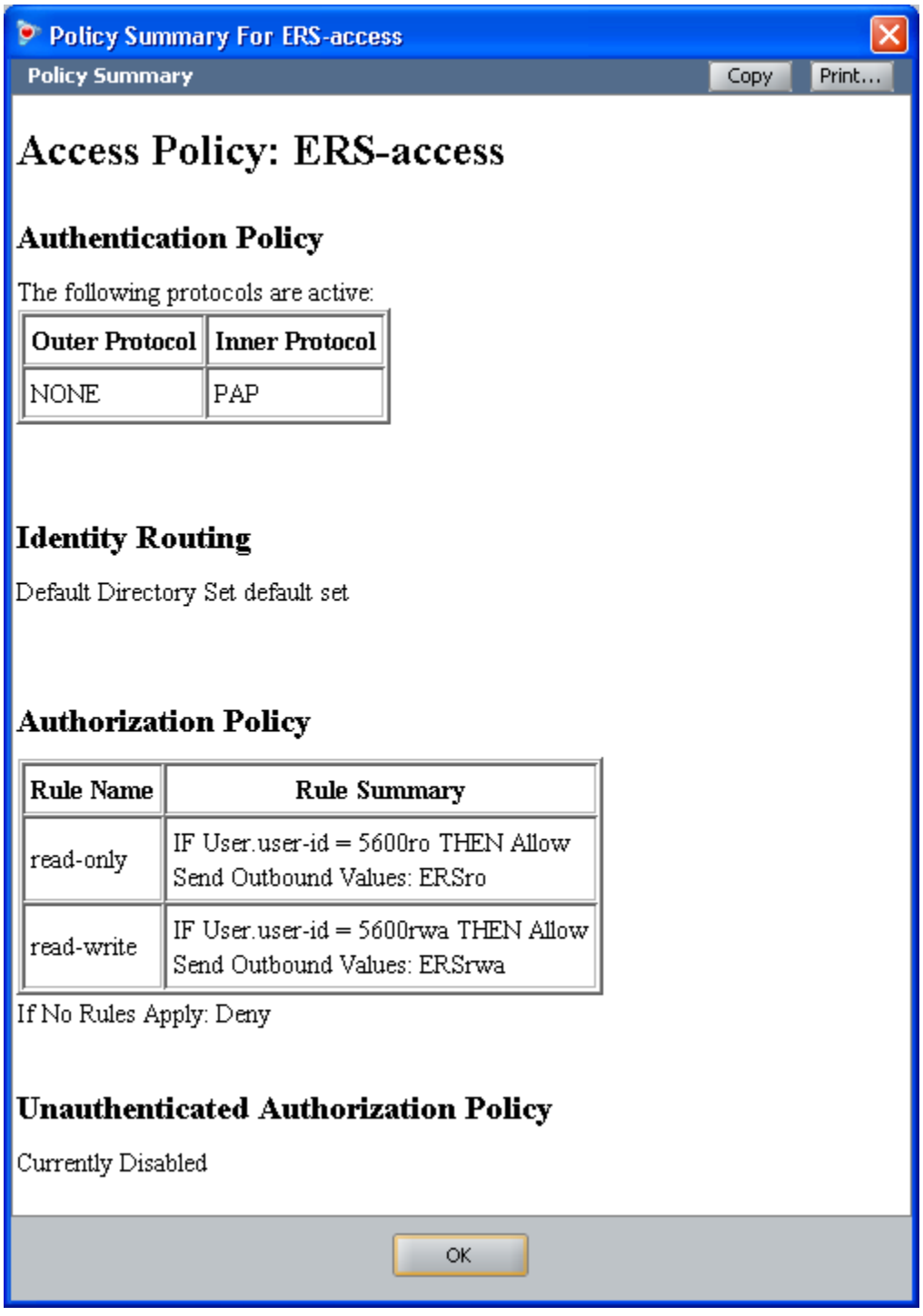
Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution

IDE Step 13 – Via *Actions*, select *Allow*. From the *All Outbound Values* window, select the output attribute we created above named *5600rwa* and click on the less-than arrow key to move the attribute to the *Provision With* window



 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 18 – When completed, you can view the complete policy by clicking on the *Access Policy Summary* button

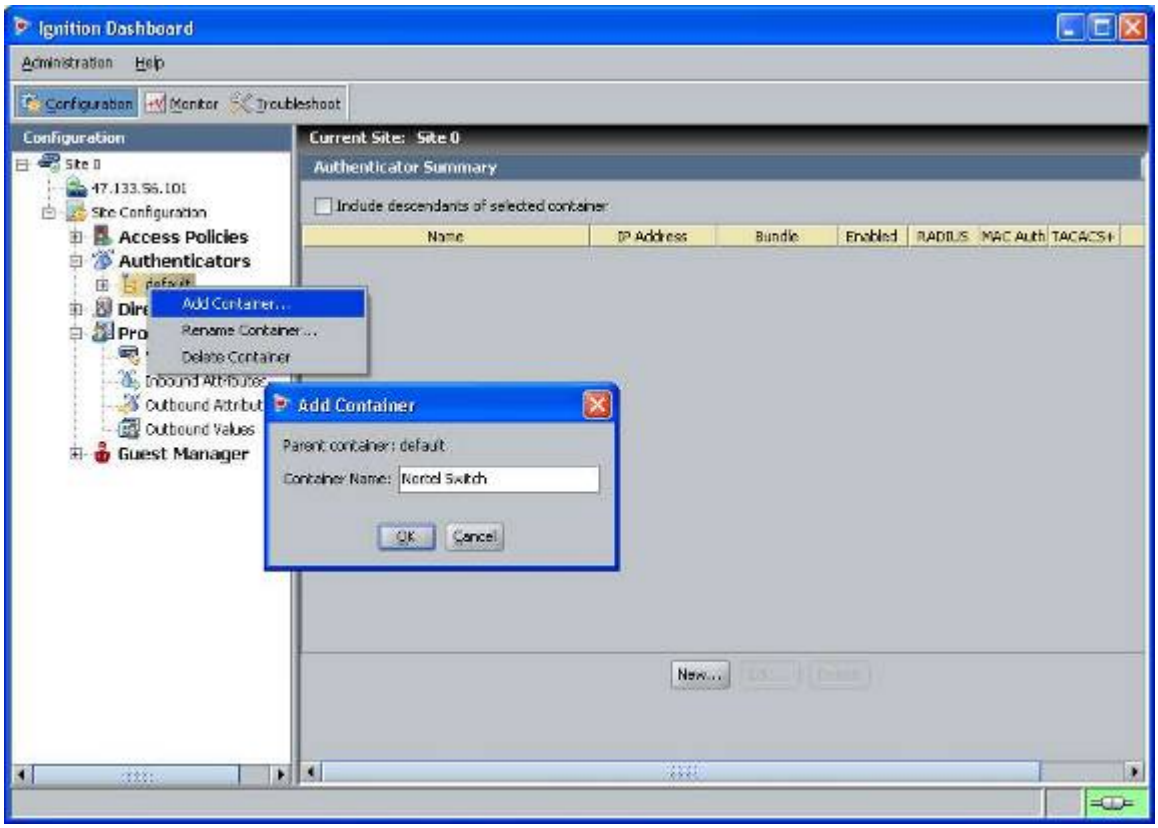


 Copyright © 2009 Nortel Networks. All Rights Reserved.

3.2.4 Add the Nortel ERS5600-1 switch as an RADIUS Authenticator

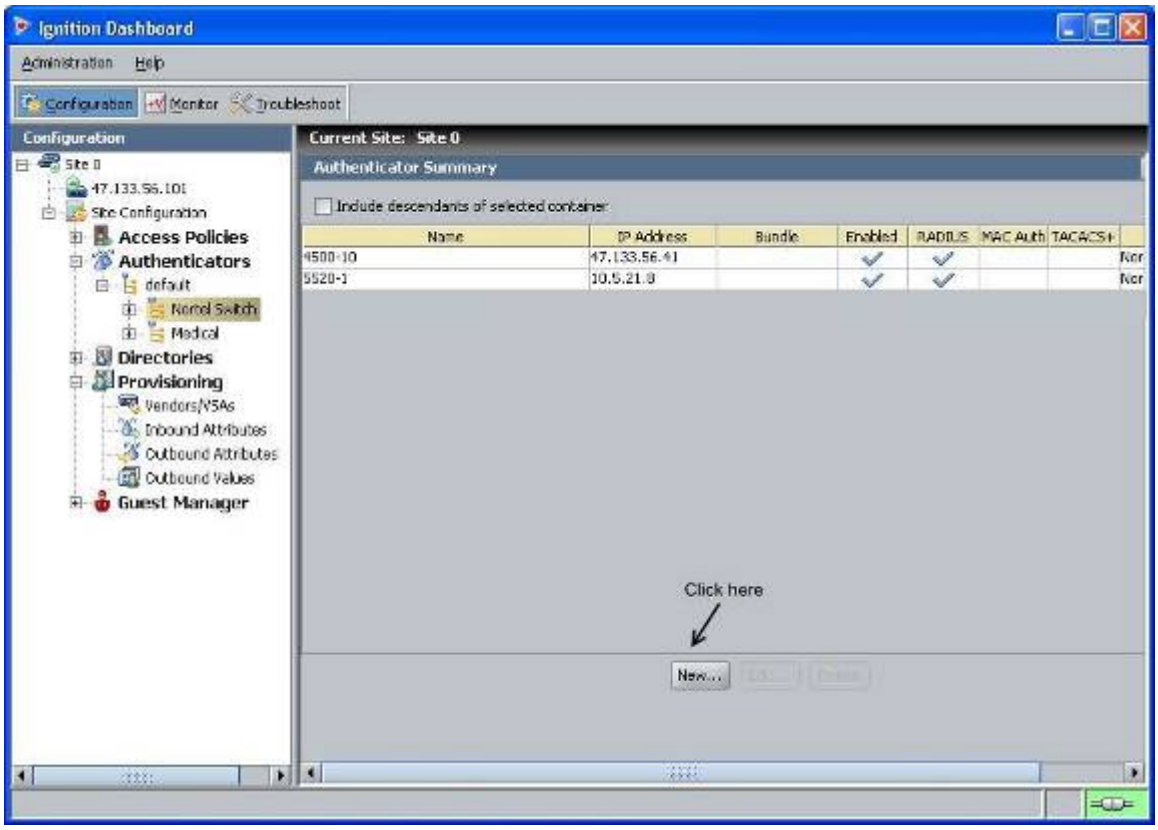
For Ignition Server to process the Nortel switch RADIUS requests, each switch must be added as an Authenticator.

IDE Step 1 – Go to *Site Configuration -> Authenticators -> default.* For example, we will create new container named *Nortel Switch* by right clicking *default* and selecting *Add Container*.



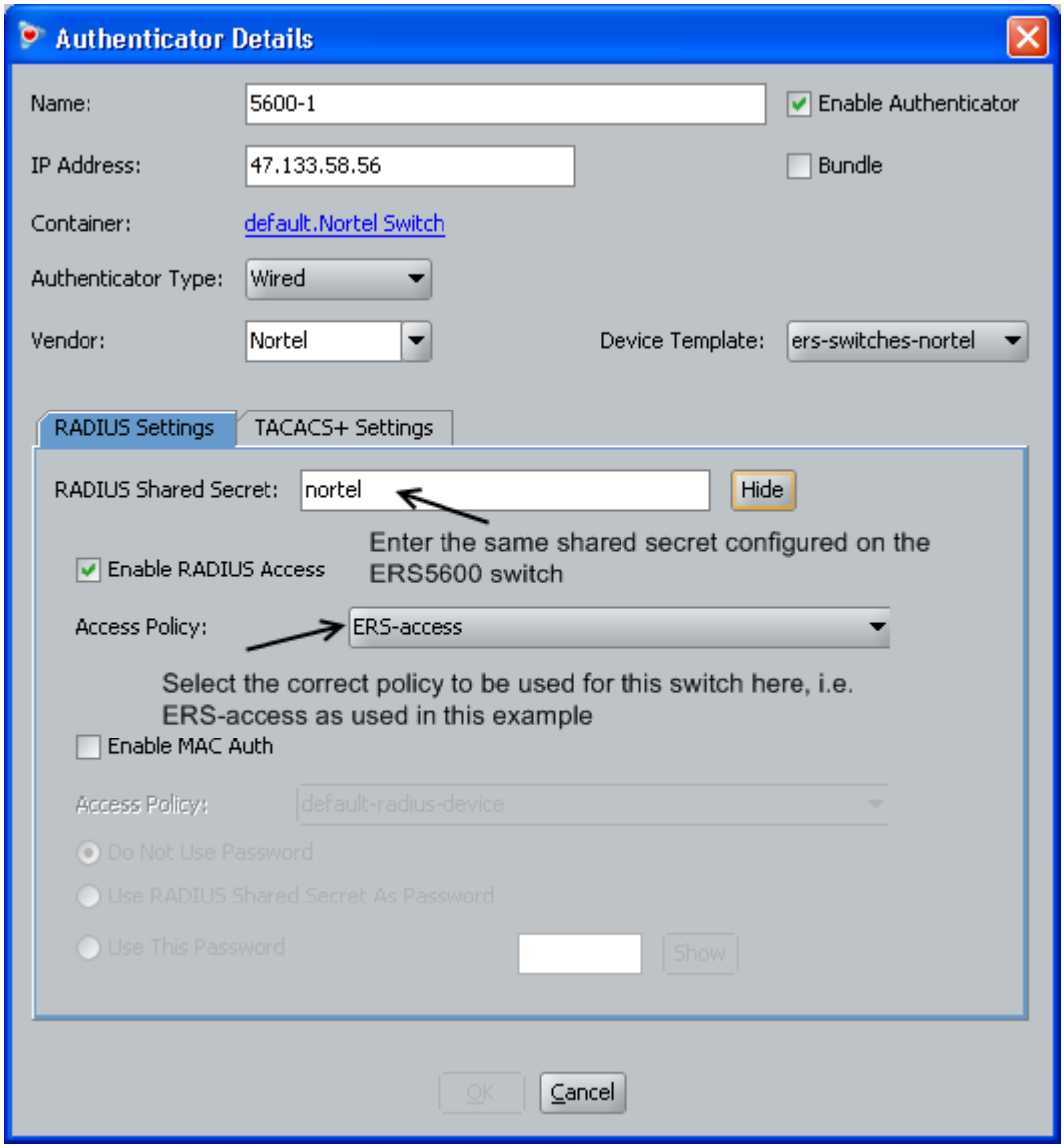
 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 2 – Go to *Site Configuration -> Authenticators -> default -> Nortel Switch* and click on *New.*



 Copyright © 2009 Nortel Networks. All Rights Reserved.

IDE Step 3 – Enter the settings as shown below making sure you select the policy we created above named *ERS-access* via *Access Policy*. Leave *Enable Authenticator* and *Enable RADIUS Access* checked. Click on *OK* when done.



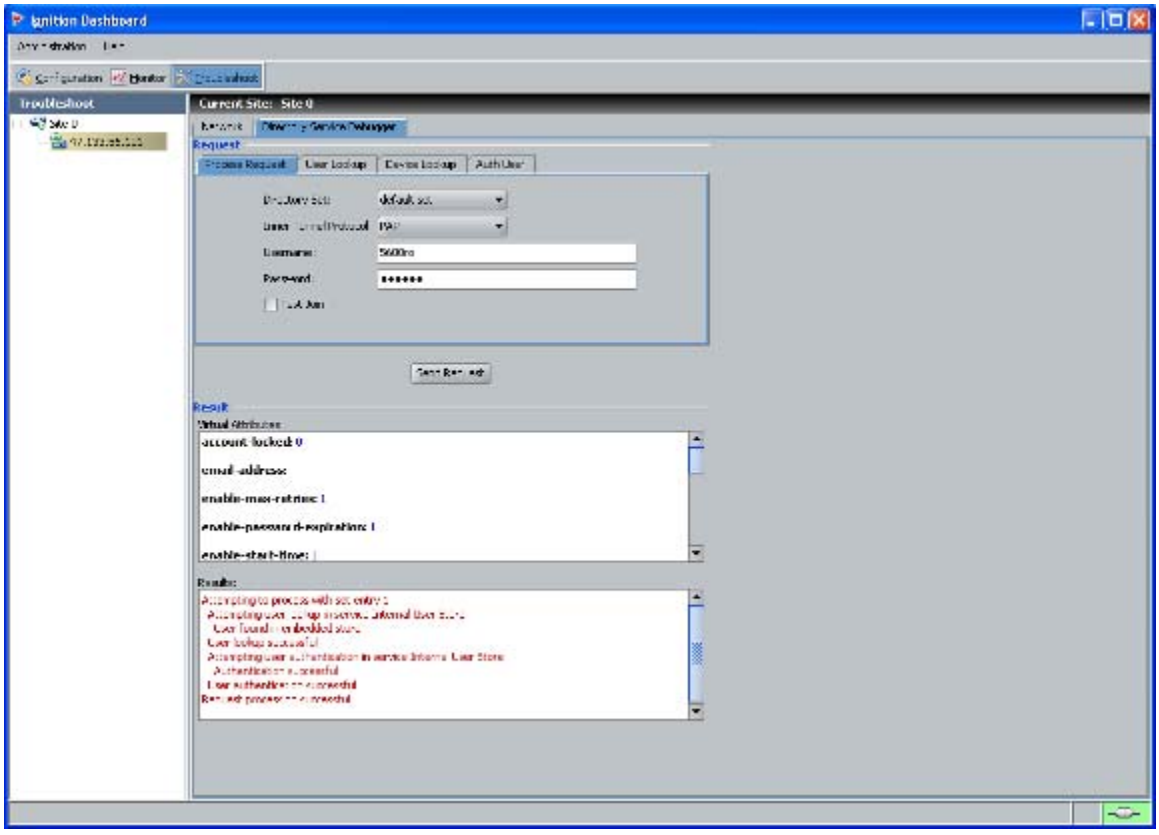
 Copyright © 2009 Nortel Networks. All Rights Reserved.

3.3 Verification

3.3.1 Verify User Authentication

You can test user authentication for the ERS5600 users configured on IDE by entering the user name and password.

Step 1 – Via Ignition Dashboard, select the IP address of the Ignition Server, click on the *Troubleshoot* tab, go to *Directory Service Debugger* and select the *Process Request* tab. You can also simple test user authentication as we did for the ERS8600 via the *Auth User* tab. Enter a valid user name and password configured for the ERS5600 and click on *Send Request*



Via Dashboard, verify the following information:

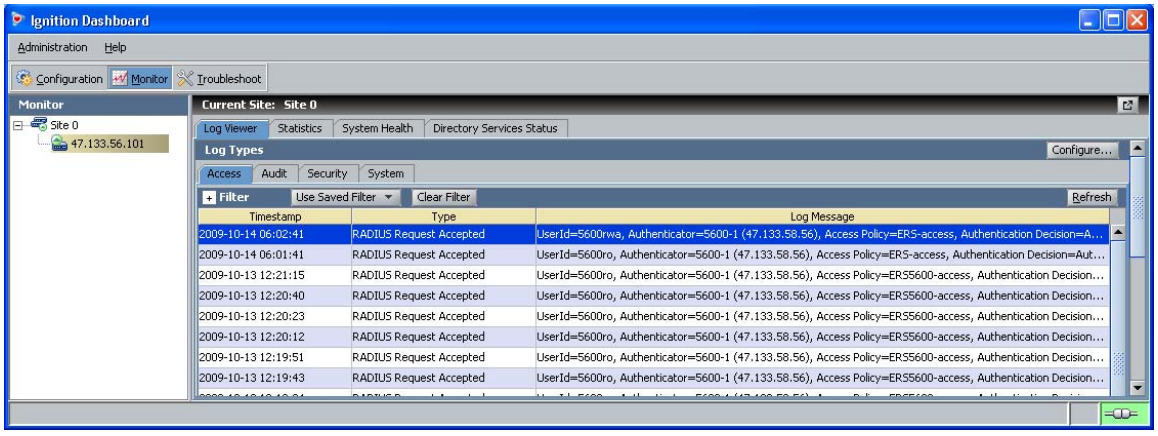
Option	Verify
Results	If successful, you should get several messages indicating the internal user lookup and authentication was successful providing you entered the correct user name and password.

 Copyright © 2009 Nortel Networks. All Rights Reserved.

3.3.2 Verify user authentication from ERS switch

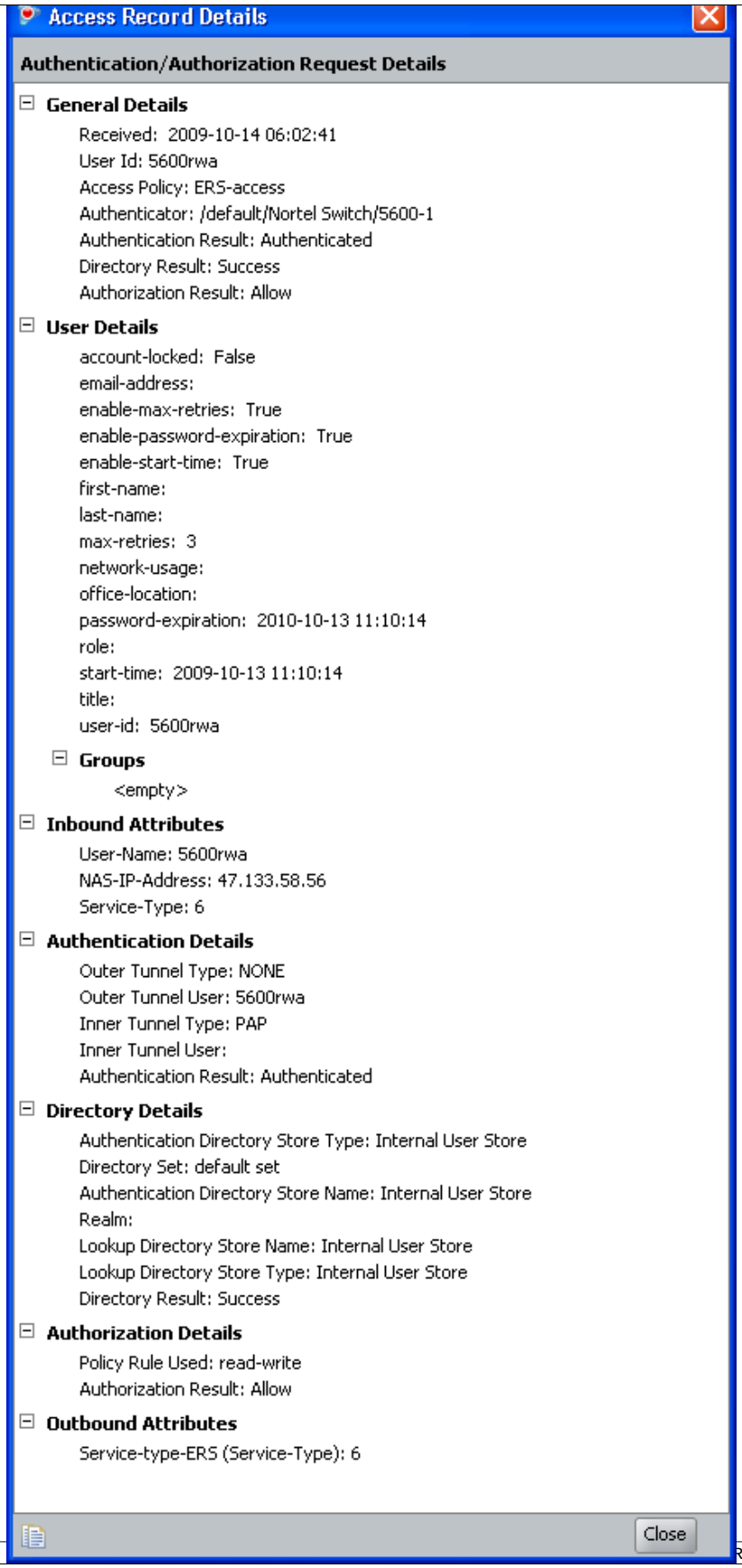
You can view the authentication details via Ignition Dashboard which provides extensive details about the device or user.

Step 1 – In Dashboard, select the IP address of the Ignition Server and click on the *Monitor* tab, go to *Log Viewer,* and select the *Access* tab. Via the message of a valid user, right-click the message and select *Access Record Details*. Shown before are the results for the read-write-all-access user. Please note you should also see RADIUS accounting records upon a user logging onto and disconnecting from the ERS5600



Result:

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.
External Distribution



Rights Reserved.

At minimum, verify the following items:

Option	Verify
Authentication Result	If successful, ***Authenticated*** should be displayed. If not, verify the device using the previous step and if this also fails, verify the Ignition Server configuration.
Authorization Result	If successful, ***Allow*** should be displayed. If not, verify the device using the previous step and if this also fails, verify the Ignition Server configuration.
User-Name	Displays the name of the user id, in this example, a user id of ***5600rwa*** was used for the user with read-write-all-access rights.
Access Policy	This field displays the Ignition Server policy used for this user which should be ***ERS-access*** as configured for this example.
Policy Rule Used Outbound Attribute	For this user, the Policy rule ***read-write*** as configured above should be used which sends an outbound vendor specific attribute value of ***6*** to the ERS8600 telling the switch this user has read-write-all-access

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.

External Distribution

4. Software Baseline

Product	Minimum Software Level
Identity Engines	6.0

.

5. Reference Documentation

Document Title	Publication Number	Description
Identity Engines Ignition Server, Release 6.0 – Document Collection	NIEIS_6.0_Doc_Collection_20090706, Rev 02	Ignition Server Software Release 6.0
Nortel Ethernet Routing Switch 2500 Series Release 4.1 Document Collection	ERS2500_4.2_Doc_Collection_20090302	Ethernet Routing Switch 2500 Software Release 4.2
Nortel Ethernet Routing Switch 4500 Series Release 5.1 Document Collection	ERS4500_5.3_Doc_Collection_20090731	Ethernet Routing Switch 4500 Software Release 5.3
Nortel Ethernet Routing Switch 5500 Series Release 5.1 Document Collection	ERS5500_6.1_Doc_Collection_20090525	Ethernet Routing Switch 5000 Software Release 6.1
Nortel Ethernet Routing Switch 8600, Release 5.1 Documentation Collection	ERS8600_5.1_Doc_Collection_20090603	Ethernet Routing Switch 8600 Software Release 5.1
Nortel Ethernet Routing Switch 8300, Release 4.2 Documentation Collection	ERS8300_4.2_DOC_COLLECTION_20090702, Rev 04	Ethernet Routing Switch 8300 Software Release 4.2
Nortel Ethernet Routing Switch 1600, Release 2.1 Documentation Collection	ERS1600_2.1_DOC_COLLECTION_20061128	Ethernet Routing Switch 1600 Software Release 2.1

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.

External Distribution

Contact us

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact Nortel Technical Support. To obtain contact information online, go to www.nortel.com/contactus.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to www.nortel.com/erc.

Nortel Confidential Information Copyright © 2009 Nortel Networks. All Rights Reserved.

External Distribution